Auditing Notes

for South African Students

Ninth Edition



Jackson & Stent

LexisNexis®

AUDITING NOTES FOR SOUTH AFRICAN STUDENTS

NINTH EDITION

JACKSON AND STENT

PREFACE TO THE NINTH EDITION

This ninth edition of the book has been compiled specifically to assist students at tertiary institutions in South Africa with their studies in auditing. The book is not designed to be used on its own and will ″work best″ when used in conjunction with the Companies Act 2008 and its Regulations 2011, the International Standards on Auditing and the (SAICA) Code of Professional Conduct. Extensive reference is made to these and other pronouncements.

The primary reason for the ninth edition is to bring the text right up to date. A number of ISAs have been revised and some changes in the SAICA (and IRBA) Code of Professional Conduct have been made. These changes are not major but needed to be dealt with.

With the increase in the number of independent review and compilation engagements which are now being undertaken by practitioners, International Standards of Review Engagements ISRE 2400 – Engagements to Review Financial Statements and International Standards on Related Services ISRS 440 – Compilation Engagements, have taken on new significance. Both of these statements have been revised and re-issued, and are covered in depth in the ninth edition.

Changes have also been made in many other chapters, mainly to address a change in legislation, provide a better illustrative example or simply to improve explanations.

Our intention has been to 'simplify' what has proved to be a difficult subject for many generations of auditing students. We hope that we have achieved this. Any comments or suggestions to improve subsequent editions would be most welcome, especially from students who use the book.

R D C Jackson B.Acc (Natal), M.Com (Rhodes), CA(SA)
Former Professor in the School of Accounting, University of KwaZulu-Natal, Durban.

W J Stent B.Com (Hons) (Rhodes), M.Com (RAU), HDE (Rhodes), PhD (Massey), CA(SA), CISA.
Former Senior Lecturer in the School of Accounting, University of KwaZulu-Natal, Durban.

Copyright subsists in this work. No part of this work may be reproduced in any form or by any means without the publishers written permission. Any unauthorised reproduction of this work will constitute a copyright infringement and render the doer liable under both civil and criminal law.

© 2014 LexisNexis
215 North Ridge Road
Morningside, Durban. 4001
www.lexisnexis.co.za
Telephone: 031 2683111

NINTH EDITION
ISBN 978 0 409 05726 3

CONTENTS

Please see the end of the book for detailed chapter by chapter index

Chapter 1	**Introduction to Auditing**	**1/1 - 1/24**
Chapter 2	**Professional Conduct**	**2/1 - 2/53**
Chapter 3	**Statutory Matters** * **Companies Act 2008 and Regulations** * **Close Corporations Act 1984** * **Auditing Profession Act 2005**	**3/1 - 3/93**
Chapter 4	**Corporate Governance**	**4/1 - 4/38**
Chapter 5	**General Principles of Auditing** * **Internal control** * **Audit evidence** * **The auditor's toolbox** * **Audit sampling**	**5/1 - 5/33**
Chapter 6	**An Overview of the Audit Process**	**6/1 - 6/23**
Chapter 7	**Important Elements of the Audit Process**	**7/1 - 7/44**
Chapter 8	**Computer Audit - The Basics**	**8/1 - 8/50**
Chapter 9	**Computer Audit - Networks and Related Concepts**	**9/1 - 9/35**
Chapter 10	**Revenue and Receipts Cycle**	**10/1 - 10/72**
Chapter 11	**Acquisitions and Payments Cycle**	**11/1 - 11/52**
Chapter 12	**Inventory and Production Cycle**	**12/1 - 12/29**
Chapter 13	**Payroll and Personnel Cycle**	**13/1 - 13/43**

Chapter 14	**Finance and Investment Cycle**	**14/1 - 14/31**
Chapter 15	**Going Concern and Factual Insolvency**	**15/1 - 15/11**
Chapter 16	**Reliance on Other Parties**	**16/1 - 16/13**
Chapter 17	**Sundry Topics** *** Initial Audit Engagements - Opening Balances – ISA 510** *** Subsequent Events – ISA 560** *** Related Parties – ISA 550** *** Audit Documentation – ISA 230** *** Specific types of Audit Evidence** **External confirmations – ISA 505** **Enquiries regarding litigation and claims – SAAPS 4** **External confirmations from financial institutions – SAAPS 6** **Written Representations – ISA 580** **Analytical Procedures – ISA 520** *** Using a Service Organisation – ISA 402**	**17/1 - 17/26**
Chapter 18	**The Audit Report**	**18/1 - 18/19**
Chapter 19	**Review Engagements and Related Service Engagements** *** Engagements to review historical financial statements** *** "Agreed upon procedures" engagements** *** Compilation engagements**	**19/1 - 19/22**

CHAPTER 1

INTRODUCTION TO AUDITING

CONTENTS

		Page
THEORY AND PHILOSOPHY OF AUDITING		
1.	What is an auditor?	1/2
2.	Why is there a need for auditors?	1/5
3.	More about assurance engagements	1/6
4.	Reasonable assurance, limited assurance and absolute assurance	1/8
THE ACCOUNTING PROFESSION		
1.	The nature of professional status	1/10
2.	Accounting bodies in South Africa	1/11
3.	Pronouncements which regulate the (auditing) profession	1/12
THE FINANCIAL STATEMENT AUDIT ENGAGEMENT		
1.	Introduction (public interest and public interest score)	1/13
2.	A model of the independent audit of the financial statements of a company	1/15
3.	The roles of the various parties	1/16
4.	The role of the Companies Act 2008 and Companies Regulations 2011	1/16
5.	The role of the Auditing Profession Act 2005	1/17
6.	The role of the International Standards on Auditing (ISAs)	1/17
7.	The role of the assertions	1/17
8.	The role of professional scepticism	1/19
9.	The role of professional judgement	1/19
SUMMARY		1/19
APPENDIX: AUDITING POSTULATES		1/20

THEORY AND PHILOSOPHY OF AUDITING

1. WHAT IS AN AUDITOR?

1.1 Introduction

No doubt we all have some idea about what an auditor is and what an auditor does, but these ideas are usually based on what we see in the media, and are often vague or clouded with misconceptions! We hear or read that the "auditors are investigating the matter", or that the Auditor General "tabled his report in parliament". On television game shows or talent shows we are told that "the auditors are standing by to verify the results" and we occasionally read in the newspaper that an "environmental audit" has been carried out for a large industrial company. Auditors seem to be involved in numerous different activities and there seem to be numerous different kinds of "auditor".

On the other hand auditors are regularly described as boring, conservative or more rudely as "little grey men (or women)" or ″bean counters″, a description which has grown out of the popular image of auditors, serious looking individuals, in their grey suits with laptops tucked under their arms! And yet, despite the slightly mocking image, there is a general acceptance that auditing is a serious business and that auditors have a very important role to play in society. So what do auditors do?
Simply stated, auditors of all types provide assurance pertaining to information prepared or presented by one party to another party with the intention of inspiring confidence in the ″fairness″ of the information which is being prepared or presented.

Example 1, Tramlines (Pty) Ltd goes to BigMoney Bank to request a loan. BigMoney Bank tells Tramlines (Pty) Ltd that before the bank can consider giving the company a loan it must provide BigMoney Bank with financial statements for the company which must be audited. In effect, BigMoney Bank is telling Tramlines (Pty) Ltd that the company can provide the financial information, but that the bank wants some ***assurance*** from a source independent of Tramlines (Pty) Ltd that the financial information provided by Tramlines (Pty) Ltd is fair. This is where the auditor comes in. The auditor will examine (audit) the information provided by Tramlines (Pty) Ltd and report to the bank on whether it is "fair". (If the auditor does not think the information is "fair", he will say so.) This assurance about the financial information submitted by Tramlines (Pty) Ltd, adds to its credibility and BigMoney Bank will be more comfortable about relying on the information when making the decision on whether to grant the loan. If the (independent) auditor states that the information is fair the bank will be more confident that granting the loan will not result in the bank suffering a loss because Tramlines (Pty) Ltd cannot repay the loan. If BigMoney Bank did not insist on ***audited*** financial information, Tramlines (Pty) Ltd could easily manipulate its financial information to deceive BigMoney Bank into granting it a loan.

Example 2. How does giving assurance relate to a television talent show and why do the promoters of the show involve auditors? The answer is that the promoter wants the results of the talent show to be ***credible***. He does not want the sponsors, participants and very importantly the public who support the show to think the results are fixed (manipulated). If this impression is given, sponsors are likely to withdraw their support and audiences (and ratings) will decline until there is no talent show. Thus, producers engage auditors, who are generally perceived by all the parties concerned to be honest, reliable and conservative, to give an opinion on whether the information (e.g. votes cast and counted, rules, etc) underlying the result was ″fair″.

In the context of the accounting and auditing profession we can express this more formally by referring to the International Framework for Assurance Engagements, which defines an assurance engagement as one "in which a practitioner expresses a conclusion designed to ***enhance the degree of confidence*** of the intended user….." (see point 3 below for a full discussion).

1.2 Types of auditor

If we consider the following types of auditor we can get a clearer understanding of what they do and what they have in common

* ***registered*** (external) ***auditors*** – auditors who express an ***independent opinion*** on whether the annual financial statements of a company, fairly present the financial position and results of the company's operations. The external auditor is ***not*** an employee of the company. The external

auditor enhances the degree of confidence which users of the financial statements will have in the information in those financial statements. Registered auditors offer their services to the public. They are described as being "in public practice" and must be registered with the Independent Regulatory Board for Auditors (IRBA).

An audit of financial statements is by no means the only ***assurance*** engagement which registered auditors conduct. As you will see later in this text, registered auditors also frequently perform review engagements, which are also assurance engagements but which provide a lower level of assurance than an audit provides.

* ***internal auditors*** – auditors who perform ***independent*** assignments on behalf of the board of directors of the company. These assignments are varied but usually relate to the evaluation of the efficiency, economy and effectiveness of the company's internal control systems and business activities and to the evaluation of whether the company has identified and is responding to the business risks faced by the company. In a sense, the internal audit function helps senior management to meet their responsibilities in running the organisation by providing independent information about the company's departments, divisions or subsidiaries. The internal auditor enhances management's degree of confidence that the company's systems are functioning as intended and that the risks are being assessed and addressed. The internal auditor ***is*** an employee of the company, but must be independent of the department, division or subsidiary in which the assignment is being carried out. The organisational structure and reporting lines in the company will be designed to ensure that the internal audit function is as independent as possible. An individual is not required to be registered with a professional body to be employed as an internal auditor, but may choose to register with the Institute for Internal Auditors. Many internal auditors are chartered accountants and will be registered with the South African Institute of Chartered Accountants.

* ***government auditors*** – government auditors perform a role similar to that of the internal auditor – but within government departments. They will evaluate and investigate the financial affairs of government departments, reporting their findings to senior government. They assist government in meeting its responsibilities in running the financial affairs of the country and increase the degree of confidence which the government has in its departments and indirectly, the confidence which the public has in the government's financial management. The government auditor (called the Auditor General), is an employee of the government but again his status and organisational positioning makes his office ***independent*** of the government departments in which assignments are carried out. Registration with a professional body is not required to be employed as a government auditor, but again many government auditors are registered with professional bodies.

* ***forensic auditors*** – forensic auditors concentrate on investigating and gathering evidence where there has been alleged financial mismanagement, theft or fraud. Forensic audits may be carried out in any government or business entity, but it should be obvious to you that the forensic auditor needs to be ***independent*** of the entity under investigation. Where an independent and competent forensic auditor has been involved, the degree of confidence which the court/investigating body has in the financial evidence, is increased. Forensic auditing is a specialist field but because of the emphasis on financial matters, most if not all forensic auditors have a background/qualification in auditing.

* ***special purpose auditors*** – these are auditors who specialise in a particular field such as environmental auditors, who audit compliance with environmental regulations, and VAT auditors who work for the South African Revenue Services and who audit vendors' VAT returns. The conclusion presented by the special purpose auditors enhance the degree of confidence which, for example, SARS will have in the "correctness" of the VAT returns audited, or a local authority will have in an environmental impact report.

What is the characteristic common to these various audit (assurance) activities? The answer is simple but very important – it is the characteristic of ***independence***. The external auditor is independent of the company, the internal auditor is independent of the department being audited and the VAT auditor is independent of the entity whose VAT returns he may be examining. Regardless of whether it is external, internal, government, forensic, VAT or any other kind of auditing, if the person

performing the "audit" is not independent of the entity being "audited", the ***assurance*** given by the auditor will be worthless.

Let's relate this to Example 1 given earlier. If BigMoney Bank is not satisfied that the auditor who was engaged by Tramlines (Pty) Ltd was independent of Tramlines (Pty) Ltd, then the bank will regard the auditors opinion on the ″fairness″ of Tramlines (Pty) Ltd's financial information as little more than worthless.

Similarly with regard to Example 2; the intention of the promoter of a television game show which makes use of an auditor to verify results, is to convey to the public and the show's sponsors, that there is no "funny business" going on with the results, and that results are not being manipulated. He wants his results and his show to have credibility and the public to be confident that the result was valid. Now, if the auditor is not independent of the game show promoter or is not perceived by the public to be independent, his opinion on the results will be worthless!

Finally, the word "auditor" is derived from the Latin word "audire" (to hear). In ancient times, accounting took place orally e.g. a servant would tell his master what he had done to protect and develop crops, land or cattle. The master would ***listen*** to such accounts of stewardship and question the servants i.e. the master was the ***listener*** or ***auditor***. As the skills of writing and bookkeeping evolved, so auditing evolved with it, growing from merely ***listening to oral accounts*** of stewardship to ***examining written records***. In many instances, masters not wishing to attend to such matters, would have appointed a trusted person ***independent*** of the stewards to "satisfy himself of the truth" of the steward's bookkeeping. The foundation for the modern auditor had been laid, e.g. shareholders (master) engage auditors (independent trusted person) to "satisfy themselves as to the fair presentation" of the directors' (stewards) bookkeeping, which is presented in the form of the annual financial statements. As business has evolved, professional accountants are required more and more to give assurance on all kinds of different information – not only financial statements. However, the basic premise of "enhancing credibility of information" and "increasing confidence of users" remains.

Note: Postulates can be regarded as the philosophical foundations of a discipline. In their text, The Philosophy of Auditing, written over 50 years ago, Mautz and Sharaf suggested a number of auditing postulates on which modern day auditing is built. A broad understanding of these postulates will increase ones understanding of the discipline and why some aspects of auditing are as they are! These postulates have been explained in the appendix to this chapter.

1.3 Which type of auditor does this text deal with?

This text deals primarily with registered auditors, the external audit of financial statements and the assurance (opinion) given for this common engagement.

However, registered auditors frequently carry out independent reviews of financial statements so this type of engagement is also regularly referred to in the text and covered in some detail in Chapter 19. The major difference between an ***audit engagement*** and a ***review engagement*** is the nature and extent of the work done and consequently the level of assurance which is given by the registered auditor. For a detailed comparison of the two types of engagement see the chart in Chapter 19.

As touched on in para 1.2, registered auditors are individuals who are referred to by the assurance engagement framework as "professional accountants in public practice" and who offer their services in auditing, accounting, taxation etc, to the public. Such individuals must be, in terms of the Auditing Profession Act 2005, registered with the Independent Regulatory Board for Auditors (IRBA).

In the context of the auditing and accounting profession, the term audit is defined in the Auditing Profession Act 2005. The term ″audit″ means:

The examination of, in accordance with prescribed or applicable auditing standards

(i) ***financial statements*** with the objective of expressing an opinion as to their fairness or compliance with an identified financial reporting framework and any applicable statutory requirements or

(ii) ***financial and other information*** prepared in accordance with suitable criteria, with the objective of expressing an opinion on the financial and other information.

The point is that the authority to conduct an audit of financial statements or financial information as defined, is restricted to registered auditors. Although other individuals may include the word auditor in their ″job description″ e.g. internal auditor, forensic auditor, environmental auditor etc, these individuals may ***not*** conduct such audits i.e. an audit as defined by the Auditing Profession Act. (Of course if say, a forensic auditor was registered with the IRBA as being in public practice he could conduct audits as defined in addition to his forensic work.)

This is similar to the laws relating to other professions. You cannot call yourself a medical doctor or an attorney without registering with the relevant professional body, who in turn will require that you are properly trained and qualified. So how is it then that a person can call himself an "internal auditor" or a "government auditor" without registering with the IRBA? The answer is simple, Sec 41 of the Accounting Profession Act specifically permits it. As for other types of auditors, such as environmental auditors, their role is to report on matters such as compliance with environmental regulations and not on the fairness of financial statements or other information presented in accordance with financial accounting frameworks. Just to make things a little more confusing, many auditors of all different types are also chartered accountants, i.e. members of the South African Institute of Chartered Accountants (SAICA). The reason for this is that qualifying as a chartered accountant provides a wide range of relevant skills which enable the individual to join commerce and industry, go into public practice or choose to be an internal auditor, government auditor, etc.

2. WHY IS THERE A NEED FOR AUDITORS?

2.1 The split between ownership and management

The need for modern day auditors, both external and internal, arose out of the natural development of owner-managed businesses into entities which were ***owned*** by people who did not ***manage*** the business. The owners provided the finance and appointed managers to run the business. The owners would require that the managers report to them at regular intervals on their stewardship (management) of the owners' money. Many of the providers of finance who, as stated, were not involved in managing the business, had neither the time nor the expertise to determine whether what they were being told by their managers, was a fair representation of the managers' stewardship. The solution was to appoint an ***independent*** person to evaluate the reports of the managers and to provide an opinion on their truth or fair presentation. The need for the ***external*** auditor was established and entrenched.

As businesses grew and became more complex, so the responsibilities of management to run the business efficiently and effectively and to satisfy shareholders expectations, became more onerous. Out of this came the birth of the ***internal audit,*** described above as a mechanism to assist management in meeting its responsibility of running the business efficiently and effectively.

The other categories of auditor have also developed out of the growth in business; Government passes laws about protecting the environment – hence the environmental audit. Businesses suffer fraud – hence the forensic audit.

2.2 Confidence in financial information

In order to maintain the confidence of those who invest in business, whether they are members of the general public or investment companies, assurance is required that the financial information produced by business organisations is reliable and credible. It is the auditor of the financial information who provides this assurance (credibility). The success of the world's capital markets hinges partially on whether investors are confident that they can rely on financial statements and other financial information to make investment decisions. Auditors (professional accountants) play a crucial role in inspiring this confidence by expressing opinions as to the fair presentation of financial information. In turn, the availability of independently audited financial information assists in:

* directing individual investors towards investments that suit their needs eg. risk, return.
* developing the economy as a whole, by ensuring that funds are directed towards those entities which provide evidence of sound management, high productivity and strong financial positions.
* enabling the government to collect taxes on an equitable basis.

* inspiring confidence in how the government handles its finances.

Remember that the ***general public*** as well as specific investing entities, have a direct interest in the economy and that the economy is aided by the availability of reliable financial information. The performance of unit trust companies, pension fund administrators, and the South African Revenue Services affects the general public directly. In turn their performance depends on reliable financial information being available to them to make sound investments, or to levy taxes. The reliability and credibility of the information they use and which they release is enhanced by its association with the auditing profession and of the accounting profession at large.

2.3 Accountability

The "auditing" profession, and here we are not restricting our discussion to registered auditors in public practice, has blossomed over the years with the emergence of internal auditing, government auditing, forensic auditing and environmental auditing, as major forces in their own right. The dominant reason for this is that the world at large requires ***accountability***. Directors must be held accountable for the way in which they run their businesses, the government must be held accountable for the way it spends taxpayers' money, and companies whose activities affect the environment must be held accountable for the way in which they adhere to environmental regulation and legislation. This has created a need for the wider ″auditing″ profession to provide an ***independent*** service which assesses and evaluates whether directors, governments etc are meeting their responsibilities. The world demands sound corporate governance and auditors play a key role in meeting this demand.

3. MORE ABOUT ASSURANCE ENGAGEMENTS

Before moving on to discussing the specifics of the audit of financial statements (the main focus of this text) we need to take a closer look at assurance in the context of auditing. For example are there such things as non-assurance engagements? Are there different levels of assurance? What distinguishes a non-assurance engagement from an assurance engagement, etc? Before we consider these questions it is necessary for us to understand the elements of an assurance engagement. These are explained in the International Framework for Assurance Engagements.

3.1 Assurance engagements.

As we saw earlier in terms of the International Framework for Assurance Engagements, an assurance engagement is one in which the professional accountant "expresses a conclusion designed to enhance the degree of confidence of the intended users, other than the responsible party, about the outcome of the evaluation or measurement of a subject matter against the criteria". Perhaps the easiest way to understand this rather tedious definition, is to break it down into its elements and relate it to the audit or review of a set of financial statements.

Elements of an assurance engagement.

Element	*Example- audit*	*Example - review*
* ***three party relationship*** • professional accountant • responsible party • intended user	• registered auditor • directors responsible for AFS • shareholders	• registered auditor • directors • shareholders
* ***a subject matter***	* financial position, results of operations etc	* financial position, results of operations etc
* ***suitable criteria***	* International Financial Reporting Standards	International Financial Reporting Standards for SMEs
* ***sufficient appropriate evidence***	* the evidence the practitioner needs to be in a position to form an opinion as to whether the financial	The evidence the reviewer needs to express a conclusion on whether anything has come to his attention which causes

	statements are free of material misstatement and are ″presented fairly″ in terms of IFRS	him to believe the financial statements are not prepared in accordance with IFRS for SMEs.
* ***a written assurance report***	* the audit opinion report on fair presentation (reasonable assurance)	The review conclusion (limited assurance)

3.2 The audit engagement

We can deduce from the chart that the ***audit*** of financial statements is an assurance engagement in which the auditor gathers sufficient appropriate evidence to ***form an opinion*** on whether the directors, who are responsible for the financial statements, have applied IFRS appropriately in presenting the financial position, financial performance, changes in equity, cash flows and disclosure notes/(subject matter). The opinion formed is then reported by the auditor to the shareholders in the audit report.

It is important to note that

* for the auditor to form an opinion on fair presentation he must have suitable criteria in terms of which to judge fair presentation. The auditor cannot just say that fair presentation has been achieved, fairness can only be judged in terms of a benchmark or standard and this is where the accounting framework comes in. The most common frameworks are IFRS and IFRS for SMEs.
* the auditor must perform the audit in the prescribed manner. How he goes about this is laid down in the International Standards on Auditing (ISAs) with which the auditor must comply in all aspects of the audit i.e. planning, risk assessment, gathering evidence and reporting.
* the audit engagement provides ***reasonable assurance***.

This is discussed below.

3.3 The review engagement

We can also deduce from the chart that the ***review*** of financial statements is an assurance engagement and is very similar to an audit engagement. In a review engagement the reviewer (who will very often be a registered auditor) gathers sufficient appropriate evidence to ***form a conclusion*** on whether anything has come to his attention which causes him to believe that the financial statements prepared by the directors are ***not*** prepared in accordance with IFRS for SMEs (or IFRS).

Again it is important to note that

* the reviewer forms his conclusion in terms of defined criteria, in this case IFRS for SMEs. (Could also be IFRS.)
* the reviewer must perform the review in the prescribed manner. How he goes about it is laid down in ISRE 2400 – International Standards on Review Engagements. Although some of the concepts or procedures in the ISAs are relevant, the ISAs are auditing standards and are not applicable to a review engagement.
* the review engagement provides only ***limited assurance.***

3.4 Non-assurance engagements.

There are many types of engagement which accountants in public practice undertake, which are not assurance engagement. These include taxation services and a wide range of advisory services relating to accounting, business performance, corporate finance, etc. These services can be classified as non-assurance engagements.

Non-assurance engagements are engagements which do not meet the definition of an assurance engagement, or do not contain the elements of assurance engagements. For example, in an advisory engagement the practitioner does not normally report to a third party, or the client may not require any assurance, or there may be no suitable criteria (benchmarks or framework) against which the subject matter of the engagement can be reliably measured. Perhaps the defining characteristic of these engagements is that the professional accountant does not express an opinion or form a conclusion on the subject matter of the engagement. Examples of

non-assurance engagements illustrate this. ***Example 1 :*** the professional accountant is engaged to compile (collect, classify and summarise) certain information for the client but is not required to comment or express an opinion thereon. ***Example 2 :*** the professional accountant is requested by a client to prepare and submit the company's tax return.

4. REASONABLE ASSURANCE, LIMITED ASSURANCE AND ABSOLUTE ASSURANCE

In terms of the assurance engagement framework, there are two types of assurance engagement a practitioner is permitted to perform i.e. a ***reasonable assurance*** engagement and a ***limited assurance*** engagement. Obviously the distinction between the two is the level of assurance (the degree of confidence) which is provided by the practitioner. It is equally obvious no doubt, that the level of assurance which the practitioner can give depends on the amount of evidence which has been gathered.

4.1 Reasonable assurance

ISA 200 – Overall Objectives of the Independent Auditor, defines reasonable assurance as a ″high but not absolute″ level of assurance. Reasonable assurance can only be given when the practitioner has gathered sufficient appropriate evidence to satisfy himself that the risk that he expresses an inappropriate opinion on the subject matter is acceptably low. In the context of an audit of financial statements this means that the auditor carries out comprehensive procedures to gather evidence so that he can express an opinion, that the financial statements are fairly presented (not materially misstated) in a ***positive*** form. The nature and extent of the audit procedures he conducts, must satisfy the auditor that the risk that he will express an opinion that the financial statements are fairly presented when in fact they are not, is low.

* ***reasonable assurance*** – audit – positive expression.
  A reasonable level of assurance is conveyed by the use of the phrase ″In our opinion the financial statements present fairly …….″

4.2 Limited assurance

Limited assurance is a level of assurance which is lower than reasonable assurance but which is still ″meaningful″ to users (ISRE 2400). It has also been described as moderate assurance. Limited assurance is given when the practitioner has gathered enough evidence to satisfy himself that the risk that he expresses an inappropriate conclusion on the subject matter is greater than for a reasonable assurance engagement, but still at an acceptably low level for the particular engagement. In the context of a review of financial statements this means that the reviewer carries out sufficient procedures to gather evidence so that he can express a conclusion in a ***negative*** form as to whether anything has come to his attention which causes him to believe that the financial statements are ***not*** fairly presented. Because limited assurance is required for a review engagement the nature and extent of procedures conducted by the reviewer will be far less comprehensive than for an audit, but the reviewer must still be satisfied that he has gathered sufficient, appropriate evidenced to support his conclusion.

* ***limited assurance*** – review – negative expression
  A limited level of assurance is conveyed by ***not*** using the phrase ″In our opinion ……″ and replacing it with ″Nothing came to our attention which causes us to believe that these financial statements do not present fairly…..″

4.3 Absolute assurance

Having read the above discussion you may be wondering why the auditor cannot ***certify*** or ***confirm*** that the financial statements are 100% correct. Why is the auditor restricted to providing reasonable assurance? By carrying out more procedures couldn't he actually confirm that the financial statements are correct? Essentially the reason that the auditor cannot certify (provide absolute assurance) is that an audit has inherent limitations which prevent the auditor from certifying or confirming the 100% correctness of a set of financial statements. ISA 200 provides the basis for the following explanation of the inherent limitations of an audit.

4.4 Limitations of an audit

* ***the nature of financial reporting.*** In the preparation of financial statements, management must apply judgement in applying the relevant reporting framework, and financial statements contain many account balances which are subjective, e.g. non-

current and current assets are directly affected by estimates (subjective) of depreciation, impairment, inventory obsolescence and bad debts respectively. It is impossible to know exactly which debtors will not pay, or which inventory will become obsolete.

* ***the nature of audit procedures.*** There are practical and legal limitations on the auditor's ability to obtain audit evidence. There is always the possibility that management may not provide complete information that is relevant to the preparation of the financial statements, and accordingly the auditor cannot be certain that ***all*** relevant information has been received. Audit procedures are not designed specifically to detect fraud, and by collusion or falsification of documentation, and other means of circumventing controls carried out by management, fraudulent transactions may go undetected and the auditor may believe that evidence is valid when it is not.

* ***audit evidence is usually persuasive rather than conclusive.*** For example, an auditor is "persuaded" that an event or transaction took place by the presence of documents or information provided by management, rather than by actually witnessing the event. The documentation could be false, and the information provided by management untrue. It is obviously impossible for the auditor to ″witness″ every transaction.

* ***the use of testing.*** On a similar note the auditor cannot examine every single transaction which has taken place in the business due to financial and time constraints, therefore it is necessary to "test" check i.e. perform procedures on only a sample of transactions and balances. Once the auditor "test checks", he cannot state that everything is 100% correct, only a reasoned opinion based on the sample on which procedures were undertaken, can be given.

* ***the inherent limitations of accounting and internal control systems***. The auditor is obliged to place reliance on the systems which the client has put in place to provide financial information; these systems have inherent limitations which may result in the failure to detect errors or fraud (see "limitations of internal control", Chapter 5) and hence the information on which the auditor forms an opinion, may be flawed.

* ***timeliness of financial reporting and the balance between benefit and cost.*** To be of any value the audit opinion must be reported within a reasonable time after the financial year-end, and the benefit derived from the audit must exceed the cost. To meet these practical requirements will generally lead to some compromise in the audit, but it is compromise which users understand and accept.

* ***other matters that affect the inherent limitations of an audit.*** There are frequently aspects of the audit or assertions in the financial statements which are inherently difficult for the auditor to gather sufficient appropriate evidence and which compound the limitations of the audit. For example in some situations it is virtually impossible for the auditor to
  - determine the presence or effect of fraud conducted by senior management
  - satisfy himself that all related parties and related party transactions have been identified and correctly treated in the financial statements
  - determine the level of non-compliance with laws and regulations which may have an impact on the financial statements
  - identify and evaluate future events which may have a bearing on the going concern ability of the company

  The point is that these ″uncertainties″ contribute to the limitations of the audit process and in turn make it impossible for the auditor to provide absolute assurance.

THE ACCOUNTING PROFESSION

1. THE NATURE OF PROFESSIONAL STATUS

Professional status is ***not*** attained merely by attaching the label "professional" to a body of practitioners. It ***is*** achieved when there is public acceptance that such a body of practitioners is worthy of recognition as a profession. Howard F. Stettler (the author of a number of auditing works) suggests that certain ***attributes*** are common to groups that are generally considered to have professional standing. These ***attributes*** may be summarised as follows:

1.1 A profession offers skills and services which are highly specialised and which require:

* particular intellectual abilities,
* mastery of a specialised body of knowledge through a formal education process,
* mastery of the application of these intellectual abilities and specialised knowledge through a practical training process.

1.2 The quality of services delivered by a profession cannot easily be evaluated by the public who rely on these services. In order to protect the public and the reputation of the profession against incompetence or unethical behaviour in the field concerned, a profession is supported by certain regulatory mechanisms which include:

* the existence of laws restricting admission to practice to those who are properly qualified.
* the existence of a strong voluntary organisation dedicated to the advancement of the profession, with primary attention devoted to improvement of the services that the profession renders.
* freedom from uninhibited competition so that practice may be carried on in an atmosphere of dignity and self-respect, with adequate opportunity for concentration on the improvement of services.
* active support of a code of ethical conduct through which the public may judge the professional stature of those in practice.

1.3 A profession and its members will also demonstrate an intellectual and ethical commitment which transcends the desire for monetary gain:

* members display an underlying service motive which is not due purely to the financial rewards which may flow as a result of the services performed,
* peer evaluation is based on factors considered to be more important than financial success.

The South African Institute of Chartered Accountants (SAICA) expresses the same attributes in a slightly different way. It states that a profession is distinguished by certain characteristics including:

* mastery of a particular intellectual skill, acquired by training and education,
* acceptance of duties to society as a whole in additional to duties to the client or employer,
* an outlook which is essentially objective and
* rendering personal services to a high standard of conduct and performance.

1.4 Equally important are the ethical principles which members of the auditing profession must abide by. As is discussed in depth in chapter 2, the SAICA and IRBA Codes of Professional Conduct lay down the fundamental ethical principles that all chartered accountants and registered auditors are required to observe as

integrity : being straightforward and honest, in all professional and business relationships
objectivity : not allowing bias, conflict of interest or undue influence of others to override professional or business judgements (impartial, independent)
professional competence and due care : maintaining professional knowledge and skill at the required level and performing work diligently in accordance with applicable technical and professional standards
confidentiality : respecting the confidentiality of client information

professional behaviour : complying with laws and regulations and avoiding action which discredits the profession.

Both ISA 200 (audit) and ISRE 2400 (review) endorse these specific fundamental principles.

2. ACCOUNTING BODIES IN SOUTH AFRICA

There are a number of accounting bodies in South Africa including the South African Institute of Chartered Accountants (SAICA), the Association of Chartered Certified Accountants (ACCA), the Chartered Institute of Management Accountants (CIMA) and the South African Institute of Professional Accountants (SAIPA). In addition, there is the Independent Regulatory Board for Auditors (IRBA) which was brought into being by the Auditing Profession Act (Act 26 of 2005), and the Institute of Internal Auditors. The dominant bodies at this stage are SAICA and IRBA and their roles are closely interlinked.

2.1 South African Institute of Chartered Accountants

SAICA is registered with the International Federation of Accountants (IFAC) and is the body which looks after the interests of its members whether they are in public practice, business, or other pursuits;

* currently to qualify as a member of SAICA, the prospective accountant must obtain a recognized qualification from an accredited university, e.g. a B.Com(Hons), pass the Initial test of Competence (ITC) examination as well as the Assessment of Professional Competence (APC) examination and serve a training contract either "outside of Public Practice" (TOPP), or "in Public Practice" (TIPP). Topp training takes place in an Approved Training Organisation (ATO) such as Investec, Angloplats, etc. TIPP training takes place in a registered training office (RTO), e.g. Deloittes or Gobodo Inc.
* an individual who satisfies the above requirements, may join SAICA and use the designation CA (SA) which stands for Chartered Accountant (South Africa)
* a member of SAICA can either be a ***chartered accountant in public practice*** or a ***chartered accountant in business.***
* a chartered accountant in public practice is an accountant in a firm (may be a sole practitioner) who provides services requiring accountancy or related skills such as auditing, taxation, management consulting and financial management services, e.g. a partner at PriceWaterhouse.
* a chartered accountant in business, is an accountant employed or engaged in such areas as commerce, industry, government service, the public sector, education, etc, e.g. a financial director at a listed company, or the financial controller in a municipality.
* a chartered accountant in public practice ***must*** be registered with the IRBA if he (or his firm) wishes to offer auditing services.

Offering accounting services such as bookkeeping, taxation, management or financial advice, is not restricted to members of SAICA. As indicated above, there are other accounting bodies such as SAIPA, ACCA or CIMA who also offer these services ***but*** members of these bodies may not offer auditing services (as defined).

Of course there is nothing to prevent an individual from being registered with two or more professional bodies provided they meet the registration requirements. The vast majority of registered auditors are members of SAICA.

2.2 The Independent Regulatory Board for Auditors

The IRBA has the responsibility of looking after the professional interests of auditors. It deals with such matters as registration, education and training, accrediting professional bodies (such as SAICA) for membership, and prescribing standards of competence and ethics. The IRBA is also there to protect the public in their dealings with registered auditors, and to discipline IRBA members who "break the rules".

To become a member of the IRBA, an individual must in essence do the following

* satisfy the educational requirements of SAICA i.e. obtain a recognized qualification from an accredited university, and pass the ITC and APC examinations
* complete a training contract in public practice (in a registered training office)
* satisfy the requirements of the Audit Development Programme subsequent to meeting the requirements for registration as a chartered accountant.

The official designation for individuals registered with the IRBA, is "registered auditor" or RA.

3. PRONOUNCEMENTS WHICH REGULATE THE (AUDITING) PROFESSION

3.1 Having discussed why there is a need for auditors and other professional accountants and the attributes of a profession, the importance of maintaining and inspiring public confidence and trust, should be obvious. It is vital that the accounting profession seeks to ensure that high standards of ethics, conduct and skill are set for, and maintained by, its members. If these standards are allowed to slip, public confidence will be undermined.

3.2 Legal and professional requirements have therefore been developed over the years to ensure that appropriate standards are set and adhered to. Indeed, ISA 200 "Overall objectives of the Independent Auditor and the conduct of an Audit in accordance with International Standards on Auditing" requires, inter alia, that the auditor

* shall comply with relevant ethical requirements, including those pertaining to independence, relating to financial statement audit engagements (contained in the relevant Codes of Professional Conduct)
* shall comply with all International Standards on Auditing.

3.3 The important legislation, regulations and standards are set out in the following pronouncements :

* The Auditing Profession Act 2005
* The Companies Act 2008 and Companies Regulations 2011
* The Constitution and By-Laws of SAICA
* The SAICA Code of Professional Conduct
* The Rules regarding Improper Conduct and the Code of Professional Conduct for Registered Auditors
* International Standards on :
  - (i) Auditing (ISA)
  - (ii) Review Engagements (ISRE)
  - (iii) Assurance Engagements (ISAE)
  - (iv) Related Services (ISRS)
* International Auditing Practice Statements (IAPS)
* South African Auditing Practice Statements (SAAPS)

Note a): The responsibility for "developing and issuing high quality standards on auditing, assurance and related service engagements, related practice statements and quality control standards for use around the world" rests with the International Auditing and Assurance Standards Board.
Note b): The audit of ***listed companies*** is also influenced by the JSE listing requirements and the King III report on Corporate Governance.

THE FINANCIAL STATEMENT AUDIT ENGAGEMENT

1. INTRODUCTION

As pointed out earlier, this book focuses mainly on engagements at which the external audit of an entity's financial statements takes place. This type of engagement is classified as an assurance engagement, and must be conducted by a registered auditor. The entity could be a company or a close corporation.
Before going any further it is necessary to establish which entities must have their annual financial statements audited and which companies qualify for an independent review instead of an audit.

1.1 The public interest

The need for auditing in its various forms is a response to the needs of society and therefore of public interest. Society and business are totally interlinked and rely on each other for their survival. If there is no business, there is no workable society and without society, there is no business – no jobs, no products, no products, no jobs! As we have already discussed, the public interacts with business in numerous ways; through employment, through pension funds, through direct or indirect ownership of shares in businesses, through trading and through making loans to purchase a house or vehicle or educate ourselves. The business world and society runs on financial information and depends on that information being accurate, fair and credible. Therefore it is in the ***public interest*** that there be a method of achieving the production and use of credible information in society. This method is the wider practice of auditing which provides the independent assurance as to the truth and fairness of financial information produced primarily by business entities.

1.2 The public interest score

For many years, in order to achieve a climate of reliable financial information, the Companies Act of the time required that all companies, large or small, public or private, had their financial statements externally audited. It was the opinion of business and the legislators that this was the right thing to do in terms of the public interest. At the same time, close corporations were not required to have their annual financial statements externally audited, despite the fact that in many cases, close corporations were larger than numerous small companies. The reason for this was simple; because close corporations were (and are) managed and owned by the same individuals (the members), there is no split between owners and managers. Managers did not have to report their custodianship to the owners and the owners did not need the protection of independent assurance as to the fairness of the financial statements because in theory they worked in the business.

However, with the introduction of the Companies Act 2008, there was a shift in thinking as regards which business entities should be required to have their annual financial statements audited. The Act introduced a new method of determining which entities required an audit of their financial statements. The decision no longer hinges around whether the entity is a company (audit) or a close corporation (no audit) but is based rather on the level of ***public interest*** in the entity. As a result, the Companies Act 2008 and its accompanying Regulations stipulate that all companies and close corporations calculate their ***public interest score*** for each financial year. As you would expect, the score is based on factors which generally determine the level of interest the public has in the entity. An entity's public interest score will be the sum of

* a number of points equal to the average number of employees during the financial year
* one point for every R1 million (or portion thereof) of turnover
* one point for every R1 million (or portion thereof) of 3rd party liability at year end
* one point for every individual who directly or indirectly has a beneficial interest in any of the company's shares/members' interests.

You will notice immediately that companies and close corporations with large labour forces and high turnovers are going to have far higher public interest scores than small companies and close corporations. The public interest score method recognises this and as a result public interest scores are broken down into three strata, i.e. 350 points and above, 100 to 349 points and less than 100 points, as indicated in the Companies Regulations. The stratum into which the entity's public interest score falls assists in determining to which level of ***assurance engagement*** if any, an entity must subject its annual financial statements.

In addition to the public interest score, there is another factor which must be taken into account in determining to which assurance engagement the entity must subject its financial statements. This factor is whether the annual financial statements are ***internally compiled*** by the entity or ***externally compiled*** by what is termed an independent accounting professional (a suitably qualified accountant who is ***independent*** of the entity whose annual financial statements are being compiled).

To complete the picture, remember that there are two types of ***assurance engagement***, i.e. an independent audit or an independent review. As we have discussed an audit is far more comprehensive than a review and enables the auditor to give a higher level of assurance on the fair presentation of the financial statements. As the objective is to create a climate of reliable financial information, particularly relating to entities in which there is a high public interest, it is logical that companies and close corporations which have a high public interest score and who compile their annual financial statements themselves, should be externally audited. Similarly, companies and close corporations with lower public interest scores and which have their annual financial statements externally compiled (independently) should not have to be audited, but could rather have their annual financial statements reviewed.

The following chart summarises this:

Public Interest Score in points	***Company***	***Close Corporations and owner managed companies***
Less than 100	Review	No assurance engagement required
100 to 349	***Audit*** if AFS internally compiled ***Review*** if AFS externally compiled	Audit if AFS internally compiled No assurance required if AFS externally compiled (Note 1)
350 and above	Audit (regardless of who compiles the AFS)	Audit (regardless of who compiles the AFS)

Note 1: It may seem strange that close corporations and owner/managed companies which have their financial statements externally compiled and have points falling in the range 100 to 349, do not require their AFS to be audited or reviewed, whilst a "normal" company in the same situation must have its AFS reviewed. This is because the Companies Act and its Regulations specifically exempt owner/managed companies and close corporations from the review requirement for its annual financial statements on the grounds that as the owners and managers of these entities are the same individuals, the external compilation adds the necessary level of credibility to the financial statements and satisfies the ***limited*** interest the public has in these entities.

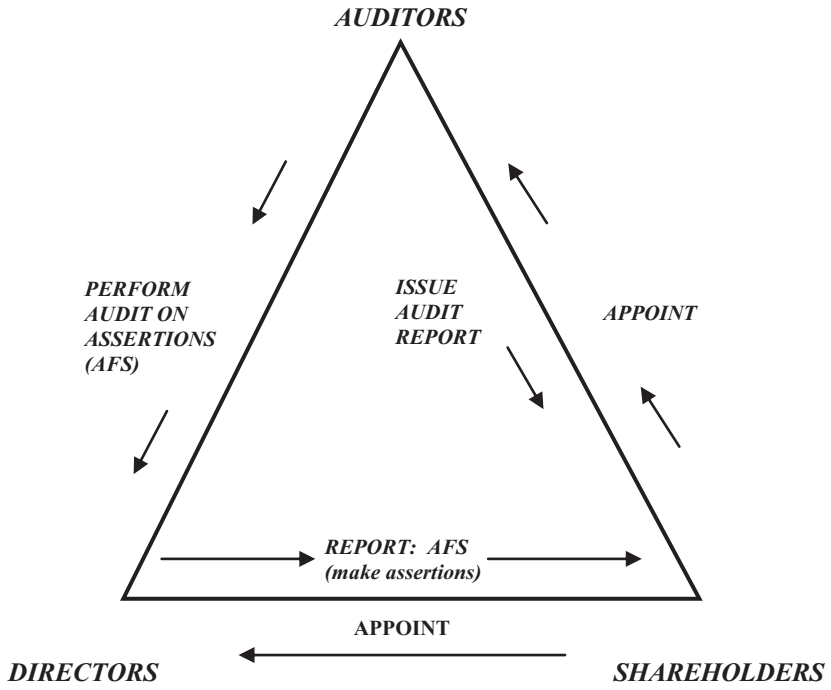
In addition to audit and review requirements arising out of public interest scores, the Companies Act 2008 and the Regulations, make it obligatory for certain other companies to have their annual financial statements audited, regardless of their public interest score. These are:

i public companies and state owned companies
ii companies which hold assets (exceeding R5m) in the ordinary course of its primary activities in a fiduciary capacity for persons not related to the company.

The reason for these specific requirements is obvious, there is a strong element of public interest.

2. *A MODEL OF THE INDEPENDENT AUDIT OF THE ANNUAL FINANCIAL STATEMENTS OF A COMPANY ARISING OUT OF THE REQUIREMENTS OF THE COMPANIES ACT 2008*

As discussed earlier in this chapter, the establishment of the modern day auditing profession arose out of the split between ownership of a business enterprise and the management of that enterprise. As businesses grew from entities owned and managed by the same person, into large private or public companies where the owners (shareholders) and managers (directors) were not the same person or persons, the need arose for an ***independent*** party (the auditor) to express an opinion on whether the reports made by those managing the business to those owning the business, were fair. Note that this is the ″three party relationship″ element of an assurance engagement. As business formalised, it became a matter of public interest to lay down rules and regulations to protect the large and small investor and the economic system as a whole. In virtually all capitalist economies, this resulted in the promulgation of "Companies Acts" by the various governments. South Africa was no exception, and for many years our Companies Act has played an integral part in the practice of auditing. The diagram and explanation presented below, illustrate the roles of the various parties and the Companies Act, in the audit.



Note (a): According to ISA 200, the overall objectives of the auditor are to:

* obtain reasonable assurance about whether the financial statements as a whole, are free from material misstatement, whether due to fraud or error, thereby enabling the auditor to express an opinion on whether the financial statements are prepared, in all material respects, in accordance with an applicable financial reporting framework (e.g. IFRS) and
* to report on the financial statements and communicate as required by the ISAs, in accordance with the auditor's findings.

Note (b): The auditor's opinion is ***not*** an assurance of the future viability of the entity, nor the efficiency with which management has conducted the affairs of the entity.

Note (c): It is ***not*** an objective of the audit to ***discover or prevent fraud*** or to ensure compliance with the law. These areas are the responsibility of management. The auditor's responsibility is to carry out his audit in such a way that there is a reasonable expectation of detecting such instances ***if*** they affect fair presentation, i.e. the financial statements contain material misstatement arising from fraud or error.

Note (d): Although this model and diagram would be very similar for a review engagement there would be some important differences. The independent review engagement is covered in depth in Chapter 19.

3. THE ROLES OF THE VARIOUS PARTIES

3.1 Shareholders

* provide finance for the business,
* appoint directors to manage the business,
* appoint auditors to express an opinion on whether the assertions (representations) relating to account balances, classes of transactions and events, as well as presentation and disclosure, which are made by the directors to the shareholders in the form of the annual financial statements, are fairly presented,
* receive the annual financial statements from the directors and a report from the auditors on the fair presentation of the financial statements.

3.2 Directors

* responsible for running the company and reporting the results of their stewardship (management) to the shareholders, by way of assertions in the annual financial statements
* preparing the financial statements in terms of an appropriate financial reporting framework (e.g. IFRS).

3.3 Auditors

* responsible for gathering sufficient appropriate evidence to be in a position to give an independent opinion on whether the annual financial statements issued by the directors to the shareholders, present fairly the financial position and results of operations of the company, in terms of the applicable financial reporting framework
* reporting the audit opinion to the shareholders.

4. THE ROLE OF THE COMPANIES ACT 2008 AND COMPANIES REGULATIONS 2011

4.1 Section 30 of the Companies Act

* makes it compulsory for all ***public*** companies to be audited and
* provides the Minister (the member of the Cabinet responsible for companies) with the power to make regulations which require ***private*** companies to be ***audited***, taking into account whether it would be desirable in the public interest, having regard to the economic or social significance of the company as indicated by
  - its annual turnover
  - the size of its workforce or
  - the nature and extent of its activities.

4.2 The Minister has exercised this power by promulgating in the Regulations, the requirement for all companies and close corporations to calculate their ***public interest score***. This in turn will play a role in determining whether the company (or close corporation) must have its annual financial statements audited.

4.3 The Companies Act 2008 also

* regulates the appointment of auditors and directors, including disqualifying certain individuals from filling these roles
* places an obligation on the directors to prepare annual financial statements, stipulates some of the content, and provides legal backing for the financial reporting standards
* provides the auditor with the right of access to the company's records. Without this the auditor cannot fulfil his independent audit function
* requires that public companies appoint an audit committee and lays down the functions of the audit committee.

All of these Companies Act sections make it possible for an effective external audit to take place, making the Companies Act an integral part of the model.

5. THE ROLE OF THE AUDITING PROFESSION ACT 2005

5.1 The AP Act 2005 Sec 41, prohibits anyone who is not a registered auditor from performing the audit of an entity's financial statements.

5.2 The Act also stipulates that the individual who is responsible for the audit is identified and named the "designated auditor" (Sec 44(1)).

5.3 The Act lays down the broad conditions for conducting an audit. Section 44 states that the auditor ***may not*** express an unqualified audit opinion on the financial statements ***unless***

* the audit has been carried out free of restriction
* in compliance with applicable auditing pronouncements
* the auditor has satisfied himself of the existence of all assets and liabilities shown in the financial statements
* proper accounting records have been kept in one of the official languages
* all information, vouchers and other documents, which in the auditor's opinion, were necessary for the proper performance of the auditors duty, have been obtained
* the auditor has not had occasion to report a reportable irregularity to the IRBA
* the auditor has complied with all laws relating to the audit of the entity and
* the auditor is satisfied as to the fairness of the financial statements.

5.4 Section 45 places a duty on the auditor to report any reportable irregularity (as defined) uncovered at an audit client to the IRBA. (This is dealt with in Chapter 3.)

6. THE ROLE OF THE INTERNATIONAL STANDARDS ON AUDITING (ISAs)

6.1 The ISAs provide the standards which the auditor must attain and provide guidance on how this should be done. The ISAs do not provide detailed lists of audit procedures; this is left up to the individual auditor or audit firm. For example, Deloitte will have their particular methods of doing things and PriceWaterhouse will have their methods. Auditing is not an exact science but provided the ISAs are complied with, an audit of the appropriate quality will be achieved.

6.2 The ISAs cover the entire ***audit process***. They provide guidance ranging from preliminary engagement activities, through planning the audit, gathering sufficient appropriate evidence, and deciding on the appropriate audit opinion and reporting the opinion.

7. THE ROLE OF THE ASSERTIONS

It is important to understand at this stage what the directors are actually representing to the shareholders in the financial statements. Once that is understood, the role of the auditor becomes clear. The report from the directors to the shareholders takes the ***form*** of the annual financial statements, and the ***content*** of the annual financial statements is controlled partly by the Companies Act and more extensively by the financial reporting standards adopted by the entity. Embodied in the financial statements, are what are termed the ***assertions*** of the directors which are in effect, their representations about the company's assets, equity, liabilities, transactions and events, and disclosures.

7.1 The assertions are laid down in ISA 315 (revised) – Identifying and Assessing the risks of Material Misstatements through understanding the Entity, as follows:

Assertions about classes of transactions and events

* ***Completeness:*** all transactions or events, which should have been recorded, have been recorded,
* ***Occurrence:*** a transaction or event which has been recorded, took place and pertains to the entity,
* ***Cut off:*** transactions and events have been recorded in the correct accounting period,
* ***Accuracy:*** amounts and other data relating to recorded transactions and events have been recorded appropriately,
* ***Classification:*** transactions and events have been recorded in the proper accounts,

Assertions about account balances at the period end

* ***Existence***: assets, liabilities and equity interests exist.
* ***Completeness***: all assets, liabilities and equity interests that should have been recorded, have been recorded.
* ***Rights and Obligations:*** the entity holds or controls the rights to assets, and liabilities are the obligations of the entity,
* ***Valuation and allocation:*** assets, liabilities and equity interests are included in the financial statements at appropriate amounts and any resulting valuation or allocation adjustments (e.g. depreciation, obsolescence) are appropriately recorded.

Assertions about Presentation and Disclosure

* ***occurrence and rights and obligations***: disclosed events, transactions and other matters have occurred and pertain to the entity,
* ***completeness***: all disclosures that should have been included in the financial statements, have been included,
* ***classification and understandability***: financial information is appropriately presented and described, and disclosures are clearly expressed,
* ***accuracy and valuation***: financial and other information is disclosed fairly and at appropriate amounts.

7.2 The assertions are dealt with more extensively in Chapter 5 but in order to understand how the assertions fit into the audit model and how they relate to the auditor's role, consider the following example:

The line item below appears in the statement of financial position (balance sheet) of Tradition Ltd:

Trade Accounts Receivable	R2 782 924

What are the directors actually saying (asserting) about accounts receivable? In terms of the assertions they are representing that:

* ***all*** debtors have been included in the amount of R2 782 924, (***completeness***)
* no fictitious debtors have been included and no amounts owing by debtors have been overstated, (***existence***)
* Tradition Ltd has the right of ownership of the amounts owed by debtors e.g. the debtors have not been factored, (***rights***)
* the amount of R2 782 924 represents the amount that can reasonably be expected to be collected from debtors after making a suitable allowance for debtors who will not pay (***valuation***), and
* the accounts receivable balance, and ***all*** information relating thereto has been appropriately presented and described and clearly expressed (***presentation and disclosure assertions***).

Note that the remaining assertions, i.e. ***occurrence, cut off***, ***accuracy*** and ***classification***, do not relate to the accounts receivable balance, as they pertain to transactions or events and ***not*** to balances. This is explained further in Chapter 5.

7.3 So what is the auditor's role with regard to the assertions? A major part of the audit is the auditor's assessment of the risk that an account balance etc will be materially misstated in the AFS. The auditor conducts this assessment by considering the likelihood (risk) of material misstatement applicable to each assertion. Once this has been done, the auditor responds by conducting procedures to gather sufficient appropriate evidence to form an opinion as to whether the account balance (and collectively the AFS) are presented fairly. To put this into context of the example given above:
Whilst assessing risk relating to the ***valuation*** assertion the auditor discovers that to attract more customers the client has relaxed its credit terms. As a result the auditor considers that the trade accounts receivable may be materially overstated (misstated) because in setting the allowance for

bad debts, Tradition Ltd's management has not taken into account the fact that the company potentially has new and less creditworthy (credit terms have been relaxed) customers. The auditor's response will be to increase the procedures which he conducts on the allowance for bad debts to determine whether it is fair or materially misstated.

8. THE ROLE OF PROFESSIONAL SCEPTICISM

8.1 Professional scepticism is an attitude, and in the context of the financial statement audit engagement is the attitude which should be adopted by all members of the engagement team. It requires that members of the team approach their work with a questioning mind, and that they be alert to conditions which may indicate possible misstatement due to error or fraud, and that audit evidence is critically assessed. It also means that members of the team should not allow themselves to be "led around by the nose" by client employees, and should not simply accept at face value what they are being told or shown by the client. An auditor should remain unconvinced of the truth of a particular fact until suitable evidence to support the fact is provided.

8.2 Members of the audit team should, for example, be alert to

* audit evidence that contradicts other audit evidence obtained
* information that brings into question the reliability of documents and responses to inquiries to be used as audit evidence
* conditions that may indicate possible fraud.

8.3 Adopting professional scepticism is not an option it is a requirement. For example, even if the auditor regards management as being honest and trustworthy, the audit will still be conducted with an attitude of professional scepticism.

8.4 Adopting an attitude of professional scepticism does not allow the members of the audit team to be rude to, or dismissive of the client's personnel; the audit team's approach should remain polite, dignified and professional.

9. THE ROLE OF PROFESSIONAL JUDGEMENT

9.1 The audit of a set of financial statements is not a specific set of clearly defined procedures carried out on clear-cut facts and figures. Different circumstances arise on different audits and there is no "one size fits all" with regard to an audit. Audits give rise to uncertainties and options which must be considered and responded to by the auditor. This is where professional judgement comes into play.

9.2 Professional judgement is the application of relevant training, knowledge and experience within the context provided by auditing, accounting and ethical standards, in making informed decisions about the courses of action and options that are appropriate in the circumstances of the audit (or review) engagement.

9.3 In terms of ISA 200, the auditor is required to exercise professional judgement in planning and performing an audit of financial statements. Virtually all decisions that must be made on an audit contain an element of professional judgement. For example, professional judgement will be required in such diverse decisions as

* evaluating the integrity of the client's management
* deciding on materiality levels
* identifying and assessing risk
* evaluating whether sufficient appropriate evidence has been gathered
* drawing conclusions on the evidence obtained and deciding on the appropriate audit opinion to be given.

SUMMARY

The auditor is a professional person who plays an important role in strengthening the credibility of financial information and hence the general and investing public's confidence in the financial and economic system of the country. This role is carried out through the expression of opinions as to whether or not financial statements are, or financial information is, presented fairly.

Confidence in the reliability of the auditor's opinion can only be maintained as long as there is public acceptance that:

* auditors are a body of practitioners who demonstrate the attributes which set them apart from the general public and make them worthy of recognition as professionals; and
* the auditing profession adheres to a strict code of ethical principles.

The profession is dynamic and is constantly changing to meet the needs of the economic community and the public at large. Auditing firms have diversified into many different services, both to remain competitive and to make use of the vast pool of talent which exists within its membership. However, at the core of the profession is the irrefutable need for a professional body which provides an independent opinion on the fairness of financial information. Financial information is the lifeblood of the economy and it is vital in the interests of society (the public at large) that such information be fair and credible.

APPENDIX

AUDITING POSTULATES

The word "postulate" is best explained by considering the following definitions from the Oxford Dictionary :

> "thing(s) claimed as a basis for reasoning" ***and***
> "postulates provide a basis for thinking about problems and arriving at solutions...a starting point...a fundamental condition"

Perhaps to express it simply we can say that the auditing postulates are the very foundation on which the discipline is built. Without a foundation, nothing of permanence can be built.

1. No necessary conflict of interest exists between the auditor and management / employees of the enterprise under audit (both the client and the auditor have the same objective with regard to fair presentation).

Explanation
This postulate proposes that the auditor and the client's management share a common desire to ensure that the financial statements prepared by management, ***do*** achieve fair presentation.

This postulate assumes that management ***will not want*** to manipulate the financial statements to present a misleading account of the affairs of the enterprise, for example, to hide fraud or to present a more favourable financial picture of the company to potential investors.

Discussion
This postulate implies that if management ***do not want*** to achieve fair presentation (and thus are willing to manipulate/falsify information), it becomes impossible to perform a conventional (normal) audit.

The postulate is critical if audits are to be economically and operationally feasible, and yet its relevance and applicability is becoming increasingly questionable. In view of the ever rising evidence of financial mismanagement, theft and fraud in business and government worldwide, is it realistic to presume that management do have the desire to report business information honestly and fairly?

The auditor has traditionally been able to rely on management's integrity in the absence of contrary evidence. In the light of the alarming increase in fraud in recent years, it has become increasingly important for the auditor to evaluate management integrity with ***professional scepticism***. Indeed, the adoption of professional scepticism by the auditor is one of the requirements placed on the auditor in terms of ISA 200 – Overall objectives of the Independent Auditor and the Conduct of an audit in accordance with International Standards on Auditing. It means that the auditor can no longer take what he or she is told by management as necessarily being the truth. It means not being "led around by the nose" or blindly accepting what management or other employees tell him, and it means that the auditor cannot accept, as a basis for the audit, that this postulate holds true.

ISA 200 defines professional scepticism as "an attitude that includes a questioning mind, being alert to conditions which may indicate possible misstatement due to error or fraud, and a critical assessment of audit evidence.

2. An auditor must act exclusively as auditor in order to be able to offer an independent and objective opinion on the fair presentation of financial information.

Explanation
The auditor's opinion can ***only*** be relied upon if he is free of any bias whatsoever, i.e. ***independent***. Furthermore, for the auditor to satisfy his duty as a professional, he should devote ***all*** of his energy to performing the audit.

Discussion

The auditor has to ***be,*** and be ***seen to be,*** independent, if he is to retain credibility as an auditor. This requires that all other interests that the auditor has, which relate to an audit client, must be carefully assessed and if they affect independence, ***either*** these interests ***or*** the audit must be relinquished. Unfortunately, the relevance and applicability of this postulate is also becoming questionable as audit firms place increasing emphasis on their ability to provide clients with other services, e.g. tax, management advice and more. It is interesting to note that in the United States of America there is a strong move on the part of the regulators of the auditing profession to commit to the principle of this postulate. Major financial scandals such as the collapse of Enron one of the largest companies in the world, provided strong evidence of a total lack of independence on the part of the auditors who are alleged to have been party to, or to have had knowledge of serious financial manipulation and fraud by the company, but did nothing about it. Was this a serious matter? It led to the worldwide demise of one of the "Big 5" auditing firms, once highly regarded for its ethics and integrity. It was a serious matter!

South Africa has also reacted to the demands of this postulate. In terms of the new Companies Act 2008, public companies (which must be audited) must also appoint an audit committee. The audit committee in turn must approve any ***non-audit work*** which the auditor of the company is engaged to perform. This can be seen to be an attempt to focus the auditor's attention on performing the audit, not on providing other services. The audit committee must be satisfied that the auditor is independent and must state whether they are satisfied with the audit of the annual financial statements. The committee is likely therefore to be very careful about what other non-audit work is given to the auditor.

3. The professional status of the independent auditor imposes commensurate professional obligations

Explanation

Professional status implies that the auditor has qualities, knowledge and capabilities which set him apart from the general public, but that this status brings with it, responsibility.

Discussion

To enjoy this status, a professional has to live up to certain expectations and accept certain responsibilities. The concepts of ***due care, service before personal interest, efficiency and competence*** flow from these expectations and have to be accepted as responsibilities by professional accountants.

4. Financial data is verifiable

Explanation

This postulate proposes that it is ***possible*** to verify the client's financial data. If this were not the case, it would be impossible to perform an audit. "Verify" means to determine something's truth or falsity, which is essentially what an audit is all about, and it implies that there will be sufficient appropriate evidence to support the transactions which have taken place.

Discussion

An auditor cannot meet the audit objective of forming an opinion on fair presentation of the financial information, unless he has gained the necessary level of assurance through verification of the financial information. With the advent of paperless transactions, trading on the Internet and E-Commerce, this postulate is increasingly under threat, as transactions may not necessarily be supported by documents which the auditor can see and touch or even access. To respond to this, the profession will need to develop new ways of gathering sufficient appropriate evidence to verify client data. Obviously if financial data is not verifiable an opinion on its fair presentation cannot be given.

5. Internal controls reduce the probability of errors and irregularities

Explanation
Simplistically expressed, internal controls are those policies and procedures which a business puts in place to ensure that its recorded transactions are valid, accurate and complete, that its assets are secured and that it complies with the law.
The postulate suggests that errors and irregularities become ***possible*** rather than ***probable*** where internal controls are good. For example, where there is a sound control environment, good division of duties and effective authorisation procedures (all internal controls) the probability of unauthorised transactions is significantly reduced.

Internal controls provide the auditor with a starting point when conducting an audit. In terms of this postulate, the better the internal controls, the more chance there is that the financial information produced will be "truthful", i.e. valid, accurate and complete. The postulate also suggests to auditors that they should realise, and make use of, the benefits of good internal control. Indeed auditing standards require that the auditor assess the effectiveness of the client's internal controls in planning the audit.

Discussion
This postulate is of critical importance to the economic and operational feasibility of audits. The alternative (i.e. no effective internal control), is a situation where auditors are forced either to refrain from offering an opinion, or to conduct extremely detailed audit examinations. Such alternatives are neither constructive, economical nor feasible. Expressed simply, without internal control the audit function is not possible. In effect if a company has very poor internal control, the financial data produced by the accounting system is most unlikely to be verifiable. (see postulate 5).

6. Application of generally accepted accounting practice results in fair presentation

Explanation
This postulate proposes that the application of generally accepted accounting practice does result in fair presentation. It suggests that there are frameworks available (***e.g. IFRS***) which, if adhered to, will result in fair financial presentation.

Discussion
This postulate emphasises the importance of objectivity and of having to measure "fair presentation" against a predetermined accepted standard. The auditor's opinion should be based on something which has gained general acceptance, rather than mere personal preferences. An accounting framework provides the auditor with a "ready made standard" against which to judge the fairness of the financial information under audit. The implication is that if the auditor obtains evidence of the proper application of appropriate generally accepted accounting practice, fair presentation will have been achieved.

7. That which held true in the past will hold true in the future (in the absence of any contrary evidence)

Explanation
As a basic premise, the auditor may assume that in the context of an ongoing audit engagement at the same client "things generally stay the same". Thus historical evidence is crucial. Judgements about the future are continually being made and accounted for on the basis of historical information. For example, when an auditor evaluates the allowance which a client has made for bad debts, to determine whether it is fair, he will take into account such matters as

* the payment records of debtors in prior years,
* the allowances which were made in prior years and
* the kinds of debtors which had to be written off in prior years.

A more general application of this postulate might be that the auditor may assume, in the light of no contrary evidence, that the integrity of the client's directors does not alter from year to year.

Discussion

The auditor has to draw on past experience when assessing judgements about the future. Factual historical evidence is far more powerful than speculation. However, this should not be taken to mean that things don't change; e.g. the integrity of the directors may decline forcing the auditor to rethink the extent to which he can rely on the representations of management in the gathering of audit evidence. Trading conditions can change in a host of different ways and new business risks may arise; the auditor must recognise this in planning and performing the audit.

8. The financial statements submitted to the auditor for verification are free of collusive and other unusual irregularities

Explanation

This postulate suggests that the auditor can start from the basic premise that the financial statements do not contain misstatement which has arisen out of collusion or similar deceptions by management. Collusion implies that there has been a deliberate attempt to misstate the financial statements. However, in terms of this postulate the auditor may, in the absence of evidence to the contrary, assume that management have taken adequate steps to ensure that the financial statements are free of "collusive or unusual irregularities" engineered by employees ***and*** that members of the management team itself have not colluded in the presentation of the financial statements.

Discussion

A cynical view may be that when these postulates were proposed (circa 1961), directors and employees were more honest than they are today! Whether this postulate holds true today could no doubt be debated at length, but the intense focus on corporate governance and the introduction of professional scepticism as an important prerequisite for auditors, suggests that this postulate is also under threat. However, for the auditor to assume the opposite i.e. that the financial statements are ***not*** free of "collusive and other irregularities" would change the objective and focus of the auditor from forming an opinion on fair presentation to an all out search for fraud and other irregularities.

CHAPTER 2

PROFESSIONAL CONDUCT

CONTENTS

		Page
The SAICA and IRBA Codes of Professional Conduct		2/3
General guidance: Ethics and Professional Conduct		2/3
The Public Interest		2/4
THE SAICA CODE OF PROFESSIONAL CONDUCT		2/5
Structure of the Code		2/5
PART A – GENERAL APPLICATION OF THE CODE		2/5
Section 100	Introduction and fundamental principles	2/5
Section 110	Integrity	2/6
Section 120	Objectivity	2/7
Section 130	Professional competence and due care	2/7
Section 140	Confidentiality	2/7
Section 150	Professional behaviour	2/8
Threats		2/10
Safeguards		2/12
PART B – CHARTERED ACCOUNTANTS IN PUBLIC PRACTICE		2/13
Section 200	Introduction and examples	2/13
Section 210	Professional Appointment	2/17
Section 220	Conflicts of Interest	2/19
Section 230	Second Opinions	2/20
Section 240	Fees and other types of remuneration	2/21
Section 250	Marketing professional services	2/22
Section 260	Gifts and hospitality	2/22
Section 270	Custody of client assets	2/23
Section 280	Objectivity – all services	2/24
Section 290	Independence - audit and review engagements	2/24
	See detailed index on the following page (2/2)	
PART C – CHARTERED ACCOUNTANTS IN BUSINESS		2/46
Section 300	Introduction	2/46
Section 310	Conflicts of interest	2/48
Section 320	Preparation and reporting of information	2/49
Section 330	Acting with sufficient expertise	2/50
Section 340	Financial interests	2/50
Section 350	Inducements	2/51

DETAILED INDEX FOR SECTION 290 – INDEPENDENCE

Introduction		2/24
The conceptual approach applied to independence		2/24
Illustrative examples:		2/26
1.	Financial interests in an audit client	2/27
2.	Loans and guarantees	2/29
3.	Business relationships	2/29
4.	Family and personal relationships	2/30
5.	Employment with an audit client	2/31
6.	Temporary staff assignments with an audit client	2/32
7.	Recent service with an audit client	2/33
8.	Serving as an officer or a director of an audit client	2/33
9.	Long association of senior personnel with an audit client	2/34
10.	Provision of non-assurance services to an audit client	2/34
11.	Preparing accounting records and financial statements for an audit client	2/35
12.	Valuation services	2/36
13.	Provision of taxation services to an audit client	2/36
14.	Provision of internal audit services to an audit client	2/39
15.	Provision of information technology services to an audit client	2/40
16.	Provision of litigation support services to an audit client	2/40
17.	Provision of legal services to an audit client	2/40
18.	Recruiting senior management on behalf of an audit client	2/41
19.	Corporate finance services	2/42
20.	Fees	2/42
21.	Compensation and evaluation policies	2/44
22.	Gifts and hospitality	2/45
23.	Actual or threatened litigation between the firm and an audit client	2/45

THE SAICA AND IRBA CODES OF PROFESSIONAL CONDUCT (Effective 1 January 2014)

There are two Codes of Professional Conduct which provide ethical guidance to chartered accountants and auditors in South Africa. They are:

1. The SAICA Code of Professional Conduct for chartered accountants.

2. The IRBA Code of Professional Conduct for registered auditors.

Both of these Codes are based on, and consistent in all material aspects with the Code of Ethics for Accountants released by the International Ethics Standards Board for Accountants (IESBA) published by the International Federation of Accountants (IFAC) in May 2013. As you would expect the two "South African" codes are consistent with each other.

Why is it necessary to have two codes? The simple answer is that the majority of chartered accountants (i.e. members of SAICA) are not members of the IRBA (i.e. registered auditors) because they ***do not conduct audits***. Typically these chartered accountants are in government, commerce or industry, engaged as internal auditors, financial directors or company accountants. They become members of SAICA so as to benefit from being part of a professional body, and thus must comply with the SAICA code.

Whilst the majority of the members of the IRBA (i.e. registered auditors) are also members of SAICA (i.e. chartered accountants), it is not a requirement that to be a member of the IRBA, the individual must join SAICA. Therefore the IRBA must have its own code and must define its own rules regarding improper conduct.

As mentioned above, the two codes are very similar and are based on the same international code. One important difference is that the SAICA code, in addition to having a section which relates to ***chartered accountants in public practice***, has a separate section which deals with ***chartered accountants in business***, i.e. chartered accountants in commerce and industry etc. The IRBA obviously does not have such a section because, by definition, registered auditors are not in commerce and industry etc, they are all ***registered auditors in public practice***.

If an individual who is a member of both the IRBA and SAICA acts improperly or unethically, he can be charged in terms of both codes. Again this is perfectly logical; the IRBA disciplinary committee has the power to "punish" one of its own members but has no power to "punish" the individual in terms of the SAICA Code. That would be up to the SAICA disciplinary process.

In summary:

* the SAICA Code applies to a person who is registered with SAICA regardless of whether he is a chartered accountant ***in public practice*** or a chartered accountant ***in business***
* the IRBA Code applies to a much narrower field, i.e. those persons registered with the IRBA as ***registered auditors***
* provided an individual complies with the registration requirements of both SAICA and the IRBA, he can be a member of both bodies.

GENERAL GUIDANCE: ETHICS AND PROFESSIONAL CONDUCT

Perhaps the most crucial prerequisite for the accounting and auditing profession is the attainment of the highest level of professional ethics by its members, both singularly and collectively. Of course members of the profession must have the necessary intellectual and practical competency, but these will be worth little if respect for, and trust in the profession is eroded by members displaying a lack of professional ethics. Indeed SAICA has identified skills and ***integrity*** as the pre-eminent attributes of Chartered Accountants (SA).

The Concise Oxford Dictionary defines ethics as: "... a set of principles or morals...rules of conduct..." and "moral" is defined as: "concerned with the distinction between right and wrong... virtuous in general conduct". ***Professional conduct*** could be described as the set of principles which governs the professional and wider behaviour of accountants and auditors.

Ethics apply when a person finds it necessary to make a decision which involves moral principles, namely a choice between "good" and "bad" or "right" and "wrong". There are various sources for ethical guidance:

* in our private lives these may include our parents, religion and role models,
* in our working lives these may include codes of conduct developed by corporations, institutions and professions, in addition to senior work colleagues or individuals trained to advise in what can be very difficult ethical situations.

Different religions, races, cultures and backgrounds may see ethical issues from totally different perspectives, so it is impossible to establish one set of hard and fast rules which can be applied to all situations which raise ethical issues. So in the absence of hard and fast rules, how does a person decide whether the ethical decision they have made, is the right one? There is no simple solution, but if the answer to the following questions is ***yes,*** then the decision is probably the right one

* is the decision honest and truthful?
* in making the decision, will I be acting in a way that I would like others to act towards me?
* will this decision build goodwill and result in the greatest good for the greatest number?
* would I be comfortable explaining my decision to people who I respect for their moral values?

In effect, asking the above four questions acknowledges that a conceptual framework approach to ethics is desirable. There cannot be a rule for every situation so some other process must be available for the chartered accountant to deal with ethical issues.

Whilst individual members of the profession will no doubt be concerned with ethical issues which affect society as a whole, (the death penalty, abortion or providing jobs at the expense of environmental destruction), it will be their daily occupations which will give rise to specific ethical situations of a professional nature, e.g.

* have I acted in a truly independent manner?
* should I make use of confidential information obtained from a client, for my own advantage?
* should I report a client who may been evading tax to the authorities?

Specific guidance and a way of thinking about ethical issues is provided in the various pronouncements indicated below.

THE PUBLIC INTEREST

As we discussed in Chapter 1, the public at large relies, directly or indirectly, on members of the accounting and auditing profession in a number of ways, one such example being the reliance which third parties, such as banks and shareholders, place on ***audited*** financial statements in deciding whether to advance finance to companies. This reliance requires that the profession accept a responsibility to the public, as reliance will only continue to be placed on the profession for as long as the profession retains public confidence in its abilities. Chartered accountants and registered auditors must therefore ensure that their services are delivered in accordance with the highest ethical and professional standards. Public reliance is not only placed on members who are in public practice. Many chartered accountants fill very influential roles in the financial world and are relied upon by the public at large to perform with integrity and competence. Even though it may be indirect reliance, the public at large rely, on:

* financial executives to contribute to the efficient and effective use of their organisations resources, and to strive for the highest levels of corporate governance,
* internal auditors in both the private and government sectors, to be part of sound internal control systems that address the risks faced by business and which enhance the reliability of financial information,
* tax experts to help establish confidence and efficiency in the tax system,
* management consultants to promote sound management decision making,
* internal auditors to promote sound corporate governance and assist in fulfilling its wider mandate.

What about trainee accountants, are they bound by the SAICA Code? The answer to this question is that if you enter into a formal training contract which is registered with SAICA, such as a training contract with a firm of accountants and auditors or the Auditor General, you will be bound by the Code. The training contract which you sign will contain a clause which requires that you adhere to the Code of Professional Conduct, and should you breach the Code, you can be disciplined. For example, if you have contravened the Code by making use of confidential information obtained whilst carrying out an audit at a client, your training contract could be cancelled.

This text concentrates on the Code of Professional Conduct of the South African Institute of Chartered Accountants (SAICA). The reasons are that your current studies are probably being conducted under the auspices of SAICA through a SAICA accredited university, and that the SAICA Code is cast a little wider as it deals with chartered accountants in business as well as in public practice. No doubt many of you will end up in business and not as auditors.

CODE OF PROFESSIONAL CONDUCT (SAICA)
(Effective 1 January 2014)

STRUCTURE OF THE CODE

1. The Code is broken down into 3 parts, and each part into sections
Part A (Sections 100 to 150) - ***General application of the Code***.
Part B (Sections 200 to 291) - ***Chartered accountants in public practice***
Part C (Sections 300 to 350) - ***Chartered accountants in business***
Note that Parts A and C also apply to a person who has been admitted and registered as an associate general accountant AGA (SA).

2. A list of definitions is also provided. Where required, definitions will be included in the narrative covering the various sections.

PART A - GENERAL APPLICATION OF THE CODE

INTRODUCTION AND FUNDAMENTAL PRINCIPLES (SECTION 100)

1. Introduction

It is a distinguishing mark of the auditing and accounting profession that registered auditors and chartered accountants have a responsibility to act in the public interest (discussed on page 2/4). The chartered accountant's responsibility is not exclusively to satisfy the needs of an individual client (chartered accountant in public practice) or his employer (chartered accountant in business). The Code establishes the fundamental principles of ethical behaviour and provides a conceptual framework which the chartered accountant can apply in ethical situations.

2. Fundamental principles

The Code establishes five fundamental principles, with which chartered accountants must comply
2.1 integrity
2.2 objectivity
2.3 professional competence and due care
2.4 confidentiality
2.5 professional behaviour

3. Basis of the Code – the conceptual framework approach

3.1 The Code provides an approach which chartered accountants should adopt to ensure that they comply with the fundamental principles. Remember that this conceptual framework approach is based on the premise that, due to the diversity of ethical issues, it is not possible or desirable to have a comprehensive set of rules to identify and resolve ethical issues. It is not possible to say "Yes you can do that" or "No you can't do this" in all situations.

3.2 Therefore chartered accountants using their ***professional judgement,*** are required to

* identify threats to their compliance with the fundamental principles
* evaluate the significance of the threat and
* apply appropriate safeguards when necessary, to eliminate or reduce the threat of non-compliance to an appropriate level, and ensure their compliance with the fundamental principles is not compromised. Safeguards are necessary if an ***informed and reasonable third party***, taking into account all the specific facts and circumstances, would consider that compliance has been compromised.

3.3 To be able to apply the conceptual approach, the chartered accountant must understand the

* fundamental principles
* types of threat which may arise
* safeguards which may be applied.

4. Conflicts of interest

In the course of his profession or business activities, a chartered accountant will be faced with conflict of interest situations. These situations can give rise to threats to the chartered accountant's objectivity and his compliance with the fundamental principles of confidentiality. Breaches of the other fundamental principles may also result. Conflict of interest is dealt with in more detail on pages 2/19.

5. Ethical conflict resolution

5.1 Because ethical matters are not clear-cut and frequently do not have a single or indisputable solution, chartered accountants may be required to resolve an ethical dilemma which they face and which they must resolve so as not to breach the fundamental principles of ethical behaviour.

5.2 Initially the chartered accountant should attempt to resolve the conflict himself by

* establishing all the relevant facts
* identifying as clearly as possible the ethical issues involved, including establishing the fundamental principles threatened
* making use of the firm's/company's internal procedures e.g. discussion with senior partner (human resources) or the ethics committee of the firm and
* considering the alternative actions, e.g. should he resign from the engagement (if employed should he resign his position), change the engagement team or ignore the matter. Each option should be evaluated.

5.3 If a significant conflict cannot be resolved the chartered accountant should consider obtaining professional advice from IRBA, SAICA or from legal advisors. (If confidentiality is an issue with this, the advice can be sought on an anonymous or hypothetical basis). If a lawyer is approached, legal privilege will apply.

THE FUNDAMENTAL PRINCIPLES

1. INTEGRITY (SECTION 110)

1.1 Chartered accountants should be straightforward, honest, fair and truthful in their professional and business relationships.

1.2 Chartered accountants should not be associated with information they believe

* contains a materially false or misleading statement
* contains statements or information provided recklessly; or
* omits or obscures information where such omission or obscurity would be misleading.

1.3 If a chartered accountant becomes aware that he has been associated with such information, he must take steps to disassociate himself therefrom. Note: this may present a threat to the fundamental principle of confidentiality.

2. OBJECTIVITY (SECTION 120)

2.1 Chartered accountants should not allow bias, conflict of interest, or undue influence of others to override or compromise professional or business judgements.

3. PROFESSIONAL COMPETENCE AND DUE CARE (SECTION 130)

3.1 Chartered accountants are required to

* maintain professional knowledge and skill at a level which ensures that clients or employers (in the case of chartered accountants in business) receive competent professional service
* act diligently in accordance with applicable technical and professional standards when providing professional services.

3.2 Rendering "competent professional service" assumes the exercising of sound judgement in applying professional knowledge and skill. To maintain professional competence a chartered accountant must remain abreast of relevant technical, professional and business developments.

3.3 Acting diligently (with due care) requires that the chartered accountant act timeously, carefully, thoroughly and in accordance with the requirements of the assignment.

3.4 A chartered accountant must ensure that those working under his authority in a professional capacity, have appropriate training and supervision.

3.5 A chartered accountant must not undertake or continue with an engagement which the chartered accountant is not competent to perform ***unless*** he obtains advice and assistance which enables the chartered accountant to carry out the engagement satisfactorily.

4. CONFIDENTIALITY (SECTION 140)

4.1 Chartered accountants should ***not***

* disclose confidential information acquired as a result of a professional or business relationship, without specific authority or unless there is a legal or professional duty to do so
* use confidential information acquired as a result of professional and business relationships to their own personal advantage or the advantage of third parties.

4.2 Chartered accountants must maintain confidentiality in a social environment and must be alert to the possibility of unintentionally disclosing confidential information to friends, long-term business associates or a close family member (definition: parent, child or sibling), or an immediate family member (definition: spouse or equivalent or dependent).

4.3 A chartered accountant should attempt to ensure that staff under his or her control and anyone from whom advice or assistance is obtained in respect of an assignment, respect the duty of confidentiality.

4.4 If a relationship between a chartered accountant, a client or employer ends, the duty of confidentiality remains. (The principle also applies to information disclosed by a prospective client.)

4.5 Disclosure of confidential information is permitted when

* disclosure is permitted by law and is authorised by the client or employer (in the case of a chartered accountant in business)
* disclosure is required by law e.g.
  - providing documents and other evidence in the course of legal proceedings

- disclosing infringements of the law to the appropriate public authority, including Reportable Irregularities in terms of the Auditing Profession Act 2005

* there is a professional duty or right to disclose confidential information about a client, e.g.
  - to comply with the requirements of an IRBA quality review (where the chartered accountant's practice is being reviewed)
  - in response to an enquiry or investigation by IRBA or SAICA
  - to protect the professional interests of a chartered accountant in legal proceedings or
  - to comply with technical standards or the requirements of the COPC.

4.6 In deciding whether to disclose confidential information, a chartered accountant should consider

* whether the interests of all parties, including third parties could be unnecessarily or unjustly harmed by the disclosures if the client consents to the disclosure of information
* whether all relevant information is known and substantiated (disclosing unsubstantiated facts or incomplete information could be unfairly damaging to other parties and is unprofessional)
* whether the method or type of communication is appropriate and the recipient of the information is appropriate, e.g. going on a popular TV talk show and disclosing confidential information about say, alleged fraud at a client company would ***not*** be appropriate.

5. PROFESSIONAL BEHAVIOUR (SECTION 150)

Section 150 deals with a number of matters under the heading of professional behaviour. Much of what has been included in the section was added by SAICA to tailor the section to satisfy the needs of the South African profession. This section deals with:

* a general explanation of the principle (5.1)
* publicity, advertising and solicitation (5.2)
* being a member of more than one firm (5.3)
* signing reports (5.4)
* recruiting (5.5)
* responsibilities to colleagues (5.6)
* discrimination (5.7)

5.1 General explanation

This fundamental principle requires that chartered accountants

* comply with relevant laws and regulations
* avoid any action which the chartered accountant knows or should know that may bring discredit to the profession (act in a way which negatively affects the good reputation of the profession as judged by a reasonable and informed third party taking into account the specific facts and circumstances available to the chartered accountant at the time of his actions).

5.2 Publicity, advertising and solicitation

Chartered Accountants are entitled to market and promote themselves and their firm, but in doing so must

* not bring the profession into disrepute
* be honest and truthful and
* not make exaggerated claims for the services they offer, the qualifications they possess, or experience they have gained
* not make disparaging references or unsubstantiated comparisons to the work of others.

Publicity - the communication to the public of information about a chartered accountant or his firm or bringing his name or the firm's name to the notice of the public.

Advertising - the communication to the public of information as to the services or skills provided by a chartered accountant with a view to procuring professional business.

Solicitation - the direct or indirect approach to a potential client for the purpose of offering to perform professional work, i.e. direct mailing and cold calling. Direct mailing includes sending a brochure to a non-client who did not request it. Cold calling includes the direct or indirect approach to a potential client in person or by telephone. Solicitation is governed by the standards presented below.

None of the activities listed above is prohibited by the Code. However, the Code requires that suitable standards be applied. Key words and concepts in this regard are:

- a ***due sense of responsibility*** on the part of the chartered accountant to the profession and to the public as a whole must be achieved,
- material for the purpose of publicity, advertising, direct mailing or cold calling should be informative and objective and be in ***good taste*** (as to content, presentation and medium),
- advertisement should ***not*** state hourly rates or "prices", as this is considered misleading and undignified,
- the ***basis*** on which professional fees for services are calculated, may be stated in an advertisement.

Perhaps the key word is ***good taste***. However, it is impossible to define "good taste" as it is very subjective. The Code does not give guidance as to what would be regarded as contrary to good taste and ultimately the responsibility for the application of the requirements of this section lies with the chartered accountant.
However, previous versions of the Code have suggested that advertising, publicity or solicitation characterised by any of the following will ***not*** be in good taste

- racist
- tends to shock, or sensationalise
- offends religious beliefs
- trivializes important issues
- relies excessively on a particular personality
- derides (make fun of) a public figure, e.g. the Minister of Finance
- disparages (mocks) educational attainment
- odious (hateful, obnoxious)
- strident (loud) or extravagant
- belittles others or claims superiority

5.3 Membership of multiple firms

A chartered accountant is permitted to be a member of more than one firm of registered auditors and/or a member of any other firm which offers professional accounting services. A chartered accountant who is a member of an auditing firm and a professional services firm which is not registered with the IRBA, must ensure that the professional services firm does not perform any audit work, pretend to be registered with the IRBA or use any designation or description likely to create the impression of being a registered audit firm in public practice, e.g. the professional services firm cannot describe itself as being "a firm of public accountants", or "accountants and auditors in public practice". (Refer Sec 41 of the Auditing Profession Act 2005.)

5.4 Signing reports or certificates

A chartered accountant must not delegate to any person who is not a partner or fellow director, the power to sign audit, review, or other assurance reports or certificates which are required in terms of the law or regulation, to be signed by the chartered accountant responsible for the engagement

* this restriction may be waived in emergencies (partner may be incapacitated). If this is the case, the need for delegation must be reported to the client and to the IRBA.

In terms of the SAICA Code, when signing off a report or certificate, e.g. an audit or review report, the chartered accountant responsible for the engagement (the designated auditor in the case of an audit) should include in his signing off

i the individual chartered accountant's (registered auditors) full name
ii the capacity in which he is signing e.g. partner or director

iii the designation "chartered accountant" (registered auditor) and if the report is not set out on the firm's letterhead,
iv the name of the chartered accountant's (registered auditor's) firm.

5.5 Recruiting

* A chartered accountant must not directly or indirectly offer employment to an employee of another chartered accountant without ***first*** informing the latter
* If an employee of another chartered accountant approaches a chartered accountant for employment, in response to an advertisement or of his own initiative, the latter chartered accountant may engage the applicant but should then inform the employer.

5.6 Responsibilities to colleagues

For any profession to remain strong and to retain the public's confidence and respect, it is essential that members of that profession remain loyal to their fellow members and that they fulfil their responsibilities to those members. This does not mean that members are above criticism or that incompetence or improper conduct is condoned. It means that there is a "right" way and a "wrong" way for a chartered accountant to fulfil his responsibilities to his fellow chartered accountant. Section 150 provides the following guidance:

* a chartered accountant should attempt to promote co-operation/good relations between fellow chartered accountants, and should not act in any way which reflects negatively on fellow accountants, e.g. criticise a fellow chartered accountant irresponsibly
* chartered accountants should assist each other in complying with the Code and where necessary, should co-operate with the appropriate disciplinary authorities in applying the Code. Serious improper conduct by fellow chartered accountants should not be condoned, as this may be repeated even where the improper conduct was unintentional. This in turn will be detrimental to the welfare of the profession as a whole, if allowed to persist
* when a chartered accountant seeks to expand his practice (attract new clients), he should not do so by means which will
  - lessen the effectiveness of technical performance, e.g. offering significantly reduced audit fees just to get the audit (lowballing)
  - lessen the integrity and objectivity of assurance opinions/conclusions e.g. requesting a friend who owns a company to dismiss the existing auditor and appoint him as auditor because they are good friends,
* a chartered accountant should extend the same professional consideration and courtesy to non-members of the profession as he would to chartered accountants.

5.7 Discrimination

Finally, with regard to professional behaviour, the previous version of the SAICA Code dealt specifically with the question of discriminatory employment practices. It stated that such practices based on matters such as race, colour, religion, sex, marital status, age or origin were contrary to the Code. For example, a chartered accountant should not be denied promotion to partner of an auditing firm or be paid a lower salary on the grounds that she is a woman. Because the current Code does not deal with discrimination separately, does ***not*** mean that discrimination is no longer a breach of the Code. It most certainly is! It is a breach of the basic requirement of professional behaviour as discrimination is contrary to labour law and the Constitution. Furthermore, any chartered accountant guilty of discrimination of this nature is in breach of the fundamental principle of integrity.

THREATS

Now that the fundamental principles have been described, it is necessary to consider the circumstances which can threaten compliance with the fundamental principles. The code categorises threats as follows:

1. Self-interest threats

Threats that a financial or other interest will inappropriately influence the chartered accountant's judgement or behaviour and lead him to act in his own self-interest. For example:

1.1 A chartered accountant has shares in an audit client (objectivity).

1.2 A firm is dependent for its survival on the fees from one client (objectivity).

1.3 A member of the audit team will join the client as an employee shortly after the completion of the audit (objectivity).

1.4 The client is placing pressure on the audit firm to reduce fees (objectivity, professional competence and due care, e.g. audit team "cuts corners" to save costs).

1.5 The engagement partner obtains confidential information about the client from a meeting with the directors, which he could use to his own financial advantage (objectivity, integrity, confidentiality and professional behaviour).

2. Self-review threats

Threats that a chartered accountant will not appropriately evaluate the results of a previous service performed by the chartered accountant or by another individual in his firm, on which the chartered accountant will rely as part of a current service

2.1 The former financial accountant of an audit client, a chartered accountant, recently resigned and joined the firm which conducts the audit of his former employer. He was placed on the audit team for the current audit (objectivity and professional competence and due care).

2.2 A firm issuing an audit opinion on the financial statements of a company for which the firm has designed or implemented the internal control system (objectivity and professional competence and due care). In terms of ISA 315, the audit team must obtain an understanding of the client's internal control. There is a threat that the audit team will assume that the internal control system is sound, without evaluating it, because their firm designed it.

3. Advocacy threats

Threats may arise when a chartered accountant promotes a client's position to a point that his subsequent objectivity may be compromised, e.g.

3.1 A chartered accountant values a client's shares and then leads the negotiations on the sale of the client's company.

4. Familiarity threats

Threats which may arise when, because of a close relationship, a chartered accountant becomes too sympathetic to the interests of others; e.g.

4.1 The chartered accountant accepts gifts or preferential treatment from a client (objectivity). This type of occurrence can threaten the basis of a professional relationship.

4.2 A member of the engagement team's father is responsible for the financial data which is the subject of the audit engagement.

4.3 The audit engagement partner and audit manager have a long association with the audit client (objectivity and (potentially) professional competence and due care i.e. the audit becomes too casual and friendly.)

5. Intimidation threats

Threats which occur when a chartered accountant may be deterred from acting objectively by actual or perceived pressures, e.g.

5.1 A chartered accountant in business fails to report a fraud perpetrated by his section head because he fears he himself will be dismissed by the section head (objectivity, integrity, professional behaviour).

5.2 An audit firm is being threatened with dismissal from the engagement (objectivity).

5.3 Pressure to accept an inappropriate decision on an accounting matter, is exerted by the client's financial director on a young, inexperienced audit manager (objectivity and integrity.)

Not all threats fall neatly into the above categories! This does not mean they are not threats. They are, and must still be addressed.

SAFEGUARDS

1. Unless the threat is clearly ***in***significant, the chartered accountant is obliged to apply safeguards (actions or measures) which will eliminate or reduce the threat to an acceptable level.

2. How does the chartered accountant decide whether a threat is clearly insignificant? There is no magic formula or "hard and fast" rule. The decision

* will be a matter of professional judgement
* must take into account the public interest – if the public interest is affected, the threat is most likely to be significant
* should be one which a reasonable and informed third party, having knowledge of all relevant information, would make in the circumstances.

3. Safeguards fall into two categories

3.1 ***Safeguards created by the profession, legislation or regulation*** e.g.

* legislation such as Sec 92 of the Companies Act 2008 which prevents an individual from being in charge of an audit for more than five years. This "rotation" requirement is aimed at enhancing independence (objectivity) by addressing a potential familiarity threat.
* educational, training and experience requirements (e.g. ethics courses) for entry into the profession
* corporate governance regulations e.g. audit committee requirements
* professional standards, e.g. the assessment of client integrity before accepting an appointment
* professional or regulatory monitoring and disciplinary procedures e.g. IRBA's or SAICA's disciplinary processes
* external reviews of a chartered accountant's work, e.g. quality control practice reviews or a partner from a separate office of the firm reviewing an audit file.

Note: In a sense, these safeguards are general rather than specific. Certainly a Companies Act section may address a specific threat or threats (such as Sec 92), but these safeguards tend rather to promote an environment of compliance with the fundamental ethical principles.

3.2 ***Safeguards in the work environment*** e.g.

* leadership of the firm that stresses the importance of compliance with the fundamental principles
* policies and procedures to implement and monitor quality control on engagements
* documentary evidence that "ethical" threats were identified, evaluated and responded to in respect of an engagement
* policies and procedures designed to identify interests or relationships between the client and members of the engagement team, e.g. questionnaires to be completed by team members
* a disciplinary mechanism to promote compliance and deal with transgressions of the fundamental principles
* having the engagement teams work subjected to independent review by say, a partner not otherwise involved with the engagement
* rotating senior assurance team personnel
* a company has sound procedures which protect an employee (a chartered accountant in business) from intimidatory threats from the employee's manager.

Note 1: The above list is by no means exhaustive and there is no "hard and fast rule" about which "safeguard" fits which "threat". It is a matter of professional judgement to be exercised by the chartered accountant and his firm.

Note 2: There may be ***no*** suitable safeguard, in which case the only course open to the chartered accountant, will be to withdraw from the engagement or relationship.

PART B - CHARTERED ACCOUNTANTS IN PUBLIC PRACTICE

SECTION 200 - INTRODUCTION

1. This part of the Code relates to chartered accountants in public practice. Accountants in public practice are obliged, as explained earlier, to identify and react to any circumstances or situation which may threaten their compliance with the fundamental principles on which the profession is built.

It is important to note that threats may vary depending on the service the chartered accountant is providing. The services the chartered accountant in public practice offers can be categorised as:
assurance engagements – an engagement where the chartered accountant expresses an opinion or a conclusion which is intended to enhance the degree of confidence of a user of the information on which the opinion or conclusion has been expressed – e.g. an audit or review of financial statements or
non-assurance engagements – an engagement where the chartered accountant does not express an opinion or draw a conclusion on information – e.g. agreed upon procedure engagements or compilation engagements.

Threats to the fundamental principles may be more significant for assurance engagements than for non-assurance engagements, particularly in the case of threats to objectivity.

To illustrate, if an opinion on the fair presentation of Atco (Pty) Ltd's financial statements is given by a chartered accountant who is not truly independent of Atco (Pty) Ltd e.g. he owns shares in Atco (Pty) Ltd, the credibility of the opinion will be questionable. Holding shares in an audit client is an unacceptable threat to the chartered accountant's ***objectivity***. If however Atco (Pty) Ltd was ***not*** an audit client and the chartered accountant was asked to compile some financial information for the company, his shareholding would not present a significant risk to his ***objectivity***.

This does not mean that threats arising on non-assurance engagements can be ignored. Objectivity is only one of the five fundamental principles and whilst there may be no specific threat to objectivity in a non-assurance engagement, other principles e.g. a threat to the principle of confidentiality may be considerable in a non-assurance engagement, e.g. when the chartered accountant is advising a client on a highly sensitive merger transaction.

2. The charts on the following three pages are designed to assist you in understanding the conceptual framework approach. The examples given are nowhere near exhaustive.

3. With regard to safeguards, it is very important to remember that:

* Sound leadership in the firm and on the engagement team, is essential.
* Policies and procedures relating to compliance with the fundamental procedures must be documented and conveyed regularly to employees.
* The disciplinary mechanism must be effective.
* Firm employees should have a procedure for, and feel safe in, raising ethical issues with senior personnel e.g. staff partner.
* The client's structures e.g. audit committees, corporate governance policies, should be embraced wherever possible.

Examples of circumstances which may create threats to chartered accountants and some possible safeguards.

Neither the threats nor the safeguards are exhaustive. The intention is to illustrate the application of the conceptual framework.

Threat	*Example*	*Fundamental Principle Threatened*	*Safeguard*
Self Interest	1. Walter Wiseman an audit partner, owns 15% of the shares in Buttco (Pty) Ltd, an audit client.	1. Objectivity, Integrity, Professional Behaviour (Walter Wiseman may overlook issues that arise on audit, to protect his investment).	1. * A policy within the audit firm which prohibits partners and employees from holding shares in an assurance client. (Walter Wiseman should dispose of his investment). * A procedure for monitoring this prohibition and a disciplinary follow up for transgressors.
	2. Joe Zulu, an audit manager, has been offered a highly paid job at one of his audit clients.	2. Integrity, Objectivity, Professional Behaviour (Joe Zulu may overlook issues that arise on audit so as not to jeopardise the job offer).	2. * Removal of Joe Zulu from the audit engagement team. * Having the key audit work performed by Joe Zulu reviewed by a chartered accountant independent of the engagement. * Notifying the company's audit committee of the situation and the safeguards put in place.
	3. Fred Fasset could make a great deal of money by getting his wife to purchase shares in a listed company of which he is in charge of the audit , before the annual financial statements are released.	3. Integrity, Confidentiality, Objectivity and Professional Behaviour. (Fred Fasset would be contravening the Insider Trading Act, acting dishonestly and making use of confidential information. If his wife purchases shares, Fred Fasset's objectivity would also be compromised).	3. * Ongoing education for employees as to ethical issues, compliance with legislation etc specifically relating to listed companies. * Instant dismissal of a firm employee (Fred Fasset) for this kind of breach of the fundamental principles, and a policy which requires that transgressors of the Insider Trading Act be reported to the relevant authorities.

Threat	*Example*	*Fundamental Principle Threatened*	*Safeguard*
Self Review	1. Harris Ford, a partner in an auditing firm has been asked by a 3rd party to provide a report on a (non audit) client's computerised sales system, which he and his team had recently designed and implemented.	1. Objectivity (Harris Ford may be tempted to omit valid criticisms of the system as he designed it – he is reporting on his own work).	1. * Notifying the 3rd party of the extent of Harris Ford and his engagement teams involvement in the system design and implementation prior to accepting the engagement.
	2. Hopgood & Co writes up the accounting records of Tuis (Pty) Ltd and have been approached to perform the annual audit.	2. Objectivity (The audit firm is not independent as it will be giving an opinion on financial statements it prepared from accounting records it compiled.)	2. In effect the Companies Act 2008 provides the safeguard. * In terms of Sec 90, an individual (or firm) may not be appointed auditor if he (or his partner or employees) regularly performs the duties of accountant or bookkeeper of that company.
	3. Clarence Kleynhans, who was, for some years, the financial manager of Kambo (Pty) Ltd, recently resigned to go back into the profession. He was employed by the audit firm that holds the appointment of auditor of Kambo (Pty) Ltd and because of his knowledge of the company, it has been suggested that he be placed in charge of the audit.	3. Objectivity, Integrity and Professional Competence (As Clarence Kleynhans would be in charge of the audit of financial information some of which he would have been directly responsible for, he cannot be regarded as being independent. His integrity may also be threatened, as there could be issues in which he was involved as the financial manager, but which he does not want to be subject to audit. It is also possible that he lacks the professional competence to manage an engagement of this nature.)	3. * A firm policy which prohibits newly appointed employees such as Clarence Kleynhans (coming from a client) from being part of the audit team until, say, two years have lapsed. * Appointing him to the engagement team (so as to make use of his knowledge) but not as the manager. * Comprehensive reviews of the work he carries out if he does work on the audit. * Notifying those charged with governance of the situation ***before*** placing him on the team. Note: as the auditor should be independent and ***seen*** to be independent, the best safeguard would be to keep Clarence Kleynhans off the team.
Advocacy (this category of threat is far less common that the others)	1. Dandy Ncobo a partner in an audit firm, has been requested to negotiate the sale of Hi-Shine (Pty) Ltd, an audit client.	1. Objectivity (Dandy Ncobo may overpromote or overstate the worth of his client to get a better price, to the extent that he is perceived as not being objective in his approach to the negotiations.)	1. * A firm policy which requires that a partner independent of the client (Hi-Shine (Pty) Ltd), handle the sale negotiation. * A firm policy which limits the non-assurance services offered to assurance clients to only those which carry a minimal threat of non-compliance with the fundamental principles.

Threat	*Example*	*Fundamental Principle Threatened*	*Safeguard*
Familiarity	1. The financial director of Travel Bug Ltd has offered to take the whole audit team on an all expenses paid weekend to an exclusive game lodge. He has stated that this will become a yearly event if the audit deadline is met.	1. Objectivity and professional competence and due care (this type of situation changes the professional relationship between the audit team from professional to "familiar". In return, the financial director may expect "favours" from the audit team. The promise of future trips if the deadline is met, may threaten the objectivity, adherence to standards and due care of future audit teams who may be tempted to "overlook" audit problems to ensure the deadline is met.)	1. * A firm policy which forbids the acceptance of gifts and hospitality which are anything other than clearly insignificant. * A strict disciplinary action for any transgressions by staff, who do not adhere to this policy.
	2. Marie Lopes, the audit manager on the audit of Topaz Ltd will shortly marry Bill Brown the financial director of Topaz Ltd.	2. Objectivity (Marie Lopes will shortly have an immediate family member (spouse) who is in a position to exert direct and significant influence over the information which she will be auditing. Her independence is compromised.)	2. * Removal of Marie Lopes from the audit. * Policies and procedures within the firm which monitor specifically the independence of the firm's employees so that situations such as this are identified and can be addressed.
Intimidation	1. The financial director of Rubdub Ltd has informed Rex Randolf, the engagement partner on the audit of Rubdub Ltd that unless the audit fee is reduced by 30%, his firm will be removed from the appointment of auditor.	1. Objectivity, Professional Competence and due care and Integrity. (To retain the audit, Rex Randolf may compromise on standards e.g. do insufficient audit work, and fail to follow up problems which he is fully aware should be followed up, so as not to go "over budget" on the reduced fee).	1. * A review of the work carried out on the audit by a partner independent of the client. * quality control procedures within the firm which review the desirability of continuing professional relationships with the firm's clients. * raising the matter with the audit committee and/or other governance structures.
	2. The financial director of ProTech (Pty) Ltd is very aggressive, domineering and dismissive of the audit function and audit team.	2. Objectivity, Professional Competence and due care. (The financial director's attitude may compromise the audit team's professional judgement. They may "be bullied" into ignoring problems on the audit out of fear of the financial director.)	2. * Appointing an engagement team which consists of experienced, strong willed individuals who will behave professionally under pressure. * Quality procedures within the firm which review, the desirability of continuing professional relationships with the firm's clients. * Discussion of the situation with the client's governance structure. * Discussion of the situation with the audit committee.

SECTION 210 - PROFESSIONAL APPOINTMENT

Client acceptance

1. Responsibility

In terms of the conceptual framework, the chartered accountant in public practice is required to consider whether accepting a new client would threaten compliance with the fundamental principles.

2. Threats

2.1 The two fundamental principles most at threat are integrity and professional behaviour. These would be threatened if, for example, the client's management condoned unethical (dishonest) business practices, the client was involved in a business sector which may have a reputation for questionable business practice such as second hand car parts, or which is socially or morally questionable. This may include companies which have no regard for environment damage or which exploit their workforce.

2.2 The fundamental principle of objectivity may also be threatened. For example, in a situation where the chartered accountant is not independent of the client.

3. Safeguards

3.1 The most effective safeguard is a thorough screening of the client prior to the acceptance of the client.

3.2 Various pronouncements made by the professional body e.g. ISA 220 – Quality control for an audit of financial statements, require that firms have quality control procedures in place which address the acceptance of new clients. The firm is required to consider inter alia

* the integrity of the principle owners, key management and those charged with governance
* whether the firm and the engagement team can comply with the ethical requirements i.e. are there any independence problems, will professional behaviour be satisfied?

3.3 How this information is obtained will vary from firm to firm but usually includes

* discussion with management, the financial director, audit committee
* discussion with chartered accountants who have provided services to the proposed client in the past
* discussions with other 3rd parties e.g. bankers
* background searches of relevant databases e.g. internet searches.

Engagement acceptance

1. Responsibility

The chartered accountant is required to consider whether he (the firm) is competent to perform the proposed engagement to the required standard.

1. Threats

The chartered accountant must consider the threats to the fundamental principles of professional competence and due care (and indirectly to professional behaviour). To accept an engagement without having the competence to perform, amounts to a self-interest threat.

3. Safeguards

3.1 The obvious safeguard lies in the quality control policies and procedures adopted by the firm.

3.2 ISA 220 requires that there be procedures in place to evaluate whether the firm has the capabilities, competence, time and resources to undertake the new engagement.

3.3 The safeguards may include

* thoroughly investigating the client's business and its complexities
* ensuring that the engagement team consists of the correct mix of skills to perform to standard

* engaging experts, other auditors (after suitable screening!)
* setting realistic time frames.

Changes in professional appointment

1. Responsibility

1.1 A chartered accountant (the proposed accountant) who is asked to replace another chartered accountant in public practice (the existing accountant), or who is considering tendering for an engagement currently held by another chartered accountant, must determine whether there are any reasons, professional or otherwise, for not accepting the engagement. This will include any threats to compliance with the fundamental principles.

1.2 In addition both the proposed accountant and the existing accountant must realise that they have responsibilities to each other. For example, the existing accountant may be angry at being replaced, this does not mean he should refuse to co-operate with the proposed accountant, or criticise the proposed accountant.

1.3 The existing accountant is also bound by certain confidentiality requirements.

2. Threats

2.1 The threat to the proposed accountant is in essence the same as the threats posed by taking on a new client/accepting a new engagement. There may be threats to the proposed accountant's compliance with the fundamental principles of professional competence and due care, professional behaviour and integrity. For example, there may be a threat to professional competence if the chartered accountant does not know all the relevant facts about the proposed client.

2.2 The threat to the existing accountant is that he fails to comply with the fundamental principle of confidentiality (e.g. by divulging confidential information to the proposed accountant without client permission) and professional behaviour (by bringing discredit to the profession by for example, criticising the client he is losing or the proposed accountant.) There is also a potential threat to integrity. The existing accountant must be honest and truthful in his dealings with the proposed accountant. The threat is particularly real if the existing accountant is angry/upset about being replaced.

2. Safeguards

3.1 The safeguards which apply to accepting a new client and accepting a new engagement will apply to this situation.

3.2 In addition, the proposed accountant should effect the following safeguards

* discuss the client's affairs fully and freely with the existing accountant. It will be necessary for the proposed accountant to obtain the client's permission in writing to do so. If the client declines to give this permission, it would suggest that a significant threat will have arisen which probably cannot be addressed. What is the client attempting to hide?
* asking the existing accountant to provide any facts or circumstances of which, in the existing accountant's opinion, the proposed accountant should be aware before accepting the engagement e.g. poor relationships between the client and its professional advisors.

3.3 The existing accountant should address the threats facing the firm by implementing the following safeguards

* obtaining the client's permission to discuss the client's affairs with the proposed accountant, and defining the boundaries of what may be discussed (in writing)
* providing the proposed accountant with information honestly and unambiguously
* put a senior, experienced partner in charge of the transition to avoid the negative emotive issues from being introduced e.g. criticism, and to ensure that what can be a difficult situation, is handled professionally.

SECTION 220 - CONFLICTS OF INTEREST

1. Responsibility

A chartered accountant in public practice may be faced with a conflict of interest when performing virtually any type of professional service including audits, reviews, taxation services, advisory services including corporate finance, forensic and information technology. A chartered accountant ***cannot allow*** a conflict of interest to compromise his professional or business judgement.

2. Threats

2.1 Conflicts of interest create a threat to the chartered accountant's objectivity and may also give rise to threats to the other fundamental principles, particularly confidentiality. Such threats may arise when

Type 1: the chartered accountant provides a professional service related to a particular matter for two or more clients whose interest in respect to that matter, are in conflict ***or***

Type 2: the interests of the chartered accountant with respect to a particular matter and the interests of the client for whom the chartered accountant provides a professional service related to that matter, are in conflict.

Examples:

* Advising client A and client B at the same time where client A and client B are competing to acquire Company C (Type 1).
* Client X wants to acquire Company Z, and engages chartered accountant Y to advise on the acquisition. Company Z is an audit client of chartered accountant Y . A conflict of interest arises if chartered accountant Y has obtained confidential information from the audit of Company Z which may be relevant to the acquisition (Type 1).
* P and Q are partners but due to an ethical disagreement, wish to dissolve the partnership. Both partners have engaged chartered accountant R to advise them on the financial aspects of the dissolution (Type 1).
* Company S pays royalties to Company T. Chartered accountant V provides Company T with an assurance report on the "fair presentation" of the amount of royalties due whilst at the same time performing the royalties payable calculation on behalf of Company S (Type 1).
* Chartered accountant O advises Company Q to invest in Company R, a company in which chartered accountant O's wife has a financial interest (Type 2).
* Chartered accountant F advises a client to purchase and install an expensive suite of financial reporting software. The local agent for the installation and maintenance of the software is a company in which chartered accountant F's son is the majority shareholder and managing director (Type 2).

2.2 Generally when there is a potential conflict of interest, there will be a confidentiality threat as well. The chartered accountant will need to be mindful of exactly what information can be divulged to each of the parties involved.

3. Safeguards

When considering appropriate safeguards in a conflict of interest situation the chartered accountant will use professional judgement and in doing so, will consider whether a reasonable and informed third party, who has knowledge of all the specific facts and circumstances available to the chartered accountant at the time, would be likely to conclude that the safeguards ensure that compliance with the fundamental principles is not compromised.

3.1 The firm should have in place appropriate pre-engagement procedures which require that reasonable steps to be taken to identify circumstances which might create a conflict of interest, before accepting the engagement.

3.2 Using separate engagement teams for each of the clients involved in the matter which threatens to give rise to the conflict of interest.

3.3 Having a chartered accountant who is ***not*** involved in providing the service, review the work performed to assess whether key judgements and conclusions are appropriate.

3.4 Disclosing to all parties involved in the "conflict" situation that there is a conflict of interest and explaining the threats which arise therefrom. If any safeguards have been or will be put in place e.g. see 3.3 above, these should also be disclosed and explained. The parties should acknowledge their understanding and acceptance of the situation. (If the parties do not accept, the chartered accountant will have to decline or resign from the service which gives rise to the conflict of interest). All of the above should be documented (it should not be verbal and acceptance should not simply be implied).

3.5 With regard to confidentiality specifically, safeguards may include

* clear confidentiality and professional behaviour guidelines for members on the engagement team.
* the engagement partner emphasising the importance of confidentiality in the context of the specific engagement giving rise to the conflict of interest.
* having partners and employees sign confidentiality agreements.
* serious disciplinary consequences for any breaches of confidentiality by team members.

SECTION 230 - SECOND OPINIONS

1. Responsibility

A chartered accountant may be faced with a situation where he is asked to provide a second opinion on some aspect of work which has been carried out for an entity which is not an existing client. In this instance the chartered accountant has ethical responsibilities to himself and the other party (existing accountant).

2. Threats

2.1 This situation could give rise to a threat that the chartered accountant will fail to comply with the fundamental principle of professional competence and due care, if he is not provided with the same set of facts or evidence provided to the existing accountant. For example, the matter on which a second opinion is sought, is how a complex transaction which is subject to various conditions, should be treated in the financial statements. The chartered accountant from whom the second opinion has been sought, gives his opinion without being aware of the full extent of the various conditions. His opinion is then discredited, and he appears incompetent.

2.2 Another threat that arises is that the second opinion, if it differs from the first opinion, may appear to be a criticism of the provider of the first opinion. This is a threat to compliance with the principle of professional behaviour.

2.3 A further threat is that the client requesting the second opinion may be attempting to implicate the chartered accountant in discrediting the provider of the first opinion e.g. seeking evidence to support a court action. This would be a potential threat to the chartered accountant's compliance with integrity and professional behaviour (responsibility to colleagues).

3. Safeguards

3.1 Obtaining from the client a precise written explanation of why the second opinion is needed.

3.2 Obtaining the client's permission to contact the provider of the first opinion to discuss the matter. (If this permission is not given the chartered accountant should consider very carefully whether it is appropriate to provide a second opinion).

3.3 Committing all communications to writing and having them reviewed by a second party within the firm.

3.4 Having the entire matter handled by senior personnel only.

3.5 The firm having a policy that they will not accept "second opinion" engagements.

SECTION 240 – FEES AND OTHER TYPES OF REMUNERATION

Normal Fees

1. Responsibility

The chartered accountant is entitled to be remunerated fairly but must charge appropriate fees e.g. not overcharge or undercharge.

2. Threats

2.1 In an attempt to secure the engagement, a chartered accountant may quote a fee which is so low that it will be difficult to perform the engagement in accordance with applicable standards. This is potentially a threat to compliance with the fundamental principle of professional competence and due care and to a lesser extent, integrity (this is not an honest practice) and objectivity (the low fee may adversely influence the nature and extent of tests performed).

2.2 The quoting of a (fixed) fee for a service for which the time to be spent could vary significantly, presents the same threats.

3. Safeguards

3.1 Providing the client with the basis on which fees are charged (as opposed to a fixed quote).

3.2 Alerting the client in writing that the total time budgeted to be spent on the assignment, may vary if unexpected problems arise e.g. difficulty in resolving audit issues.

3.3 Discussing the terms of the engagement with the client e.g. with the audit committee.

3.4 Assigning appropriate time and suitably qualified staff to the engagement.

Contingent Fees

1. Responsibility

Contingent Fees (fees that are calculated on a predetermined basis relating to the outcome of the work performed or as a result of a transaction which arises from the service) are acceptable for a wide range of non-assurance engagements. The chartered accountant may charge such fees in accordance with business norms. (Contingent fees for assurance engagements are ***not*** permitted).

2. Threats

2.1 The charging of contingent fees may give rise to a self-interest threat to objectivity. The chartered accountant becomes more interested in the fee that could be earned than the quality of the service offered. There may also be a threat to integrity and professional behaviour if the chartered accountant does anything illegal or contrary to honest business practice in an attempt to maximise the contingent fee.

3. Safeguards

3.1 Obtaining in advance, a written agreement with the client as to the basis and detail of fees to be charged.

3.2 A committee within the firm which authorises all engagements giving rise to contingent fees, prior to their acceptance.

3.3 Disclosure of the contingent nature of the remuneration to intended users of the work performed.

3.4 A review by an independent 3rd party (committee) of the work performed by the chartered accountant, to counter any claims that the chartered accountant was only interested in maximising the fee.

Referral Fees/Commissions

1. Responsibility

A chartered accountant may receive or pay a fair referral fee or commission but must ensure that the payment of such fees or commission do not compromise the fundamental principles.

2. Threats

2.1 The threats that may arise are to compliance with the principles of objectivity, professional competence and due care and integrity. ***Example 1.*** The firm of Jones and Jones does not offer information technology services. Any requests they receive for IT services are referred to other firms for which Jones and Jones receives a referral fee. These fees vary from firm to firm. The threat is that Jones and Jones will refer the client to the firm that pays the highest referral fee, but which may not necessarily be the most suitable for the particular assignment. ***Example 2.*** Jones and Jones receive a 15% commission for any office equipment which OfficeMan (Pty) Ltd sells to clients of Jones and Jones which have been referred to the company by Jones and Jones. Again Jones and Jones have an interest in the transaction and may be referring clients to OfficeMan (Pty) Ltd because of the commission and not because of the suitability of OfficeMan (Pty) Ltd's products.

3. Safeguards

3.1 Disclosure to the client of any arrangements to pay or receive a referral fee and the details thereof. These disclosures should be made in advance of the transaction taking place and should be in writing.

3.2 In respect of the commission, disclosure in advance to the client that the chartered accountant has an interest in the transaction, e.g. the basis and extent of the commission to be paid to the chartered accountant by the supplier of the goods (again in advance and in writing).

3.3 A committee within the firm which authorises referrals/commissions relating to services and products.

SECTION 250 – MARKETING PROFESSIONAL SERVICES

1. Responsibility

A chartered accountant may attempt to obtain additional work through marketing his services, but has a responsibility to do so in a manner which does not discredit the profession in any way, e.g. advertise in bad taste, make extravagant claims etc. (Refer to Part A, Section 150).

2. Threats

If the chartered accountant markets his services in a manner which is dishonest, exaggerated, critical of other firms, obnoxious or not in good taste, the fundamental principles of integrity, and professional behaviour will not have been complied with. ***Example***. Rassack and Co places an advertisement in the financial press which claims that "the firm audits numerous listed companies (when they only audit one!), has the best audit approach and employs the most highly qualified staff".

3. Safeguards

3.1 A quality control procedure which requires that all proposed marketing/advertising (in whatever form) is reviewed and authorised by a suitable quality control committee within the firm.

3.2 Written communication with partners and employees as to what is acceptable and what is not acceptable in respect of promoting the firm (see Part A, Section 150).

SECTION 260 - GIFTS AND HOSPITALITY

1. Responsibility

A chartered accountant is allowed to receive gifts and hospitality from a client provided they are clearly insignificant (as might be judged by a reasonable and informed third party). However, it is very important that the chartered accountant turn down gifts/hospitality which may alter the relationship between "client and accountant".

2. Threats

Gifts and hospitality which are not anything other than clearly insignificant may threaten the fundamental principle of objectivity. ***Example 1***. The financial director of Multibike (Pty) Ltd gives the audit manager (a keen cyclist) a new road bike valued at R25 000 as a gift. This changes the relationship between the audit manager and the client, and poses the following questions. Why did the financial director do this?

Does he expect a favour in return? Has the relationship moved from "professional" to "familiar"? Does it provide the financial director with a means of intimidating the audit manager, by threatening to disclose the gift to the firm's partners? Self interest, intimidation and familiarity threats all become possible.

3. Safeguards

3.1 A policy that partners and staff are prohibited from accepting any gifts or hospitality from clients.

3.2 The acceptance of any gift or hospitality must be approved by the firm's quality control committee.

3.3 A notification to all clients that employees and partners may not accept gifts or hospitality other than any which may be clearly insignificant (could for example be included in the engagement letter/terms and conditions of the engagement).

SECTION 270 – CUSTODY OF CLIENT ASSETS

1. Responsibility

A chartered accountant may not take custody of a client's assets (money or other) unless permitted to do so by law. The chartered accountant must ensure that the assets do not come from illegal sources, are not used for purposes other than agreed to with the client, and must be kept separately identifiable.

2. Threats

2.1 The custody of a client's assets may threaten compliance with the fundamental principles of integrity, professional behaviour and objectivity. ***Example***. Ronnie Rings a chartered accountant, has been given sole authorisation to operate the bank accounts of Marjory Manoj, a wealthy client who is on an extended visit overseas. She has requested that Ronnie Rings pay her taxes, rates, electricity accounts etc, as they fall due. The threat is that Ronnie Rings may use his client's funds to enrich himself (self interest), e.g. make speculative deals from which he benefits using Marjory Manoj's money.

2.2 A further threat is that a client may be trying to launder illegal money through the firm. This presents a threat to compliance with the law (professional behaviour) and allegations of the chartered accountant being involved in dishonest practice (integrity).

2.3 The chartered accountant may be accused of misuse of client assets.

3. Safeguards

3.1 All client assets should be kept separate from firm assets (and readily identifiable) whether they be hard assets or bank accounts, e.g. client money should ***not*** be put into the chartered accountant's own bank account. (Separate accounts properly designated as client accounts should be opened, and monies deposited without delay. Bank accounts must be with entities registered in terms of the Banks Act 1990.)

3.2 Prior to accepting the assets, the firm should agree in writing as to what purposes the assets can be put.

3.3 Records which account for any movement in the value of the assets, e.g. income earned, must be maintained up to date, and should be available for inspection.

3.4 Prior to acceptance of the assets, the firm must establish that they do not come from illegal sources, e.g. obtain a written declaration from the recipient.

3.5 Establishing that any bank accounts involved, are FICA compliant.

3.6 Ensuring there are adequate safeguards (physical if necessary) for the assets.

SECTION 280 – OBJECTIVITY – ALL SERVICES

Section 280 is in effect a preamble to Section 290 which deals with Independence – Audit and Review Engagements. Even a brief glance at the SAICA Code will confirm that independence for assurance engagements is the single most important topic covered by the Code. This is not surprising as independence has been described as the "cornerstone of the profession" – if a chartered accountant provides an opinion or a review conclusion on a client's financial information but is not independent of that client, the credibility of the opinion/conclusion is severely compromised and it may in fact be totally worthless.

Section 280 confirms this but also reminds chartered accountants that objectivity must be brought to all engagements but to differing degrees. The overriding requirement is that chartered accountants do not compromise their professional judgement because of bias, conflict of interest or the undue influence of others.

SECTION 290 - INDEPENDENCE - AUDIT AND REVIEW ENGAGEMENTS

Introduction

1. As has been pointed out, the SAICA Code places a great deal of importance on independence particularly in respect of assurance engagements. This is not surprising as, by definition, an assurance engagement is one where a chartered accountant in public practice expresses an opinion/conclusion on client information to enhance the degree of confidence of third parties in that information. It is easy to understand that if the chartered accountant is not clearly independent of the client or the information, the intended increase in credibility/confidence will not be achieved.

2. Studying independence in terms of the SAICA Code with its unfamiliar terminology and long-windedness can be daunting, but the key to coping with it is to recognise firstly the importance of independence and secondly that the Code presents a conceptual framework for dealing with independence issues, which, if clearly understood, makes the task a great deal easier.

3. The SAICA Code contains two very long sections which deal with independence:

* Section 290: Independence – Audit and Review Engagements
* Section 291: Independence – Other Assurance Engagements

This text deals only with Section 290. The reasons for this are that the conceptual approach to independence applies in exactly the same way to both sections, the content of both sections is very repetitive and that your studies concentrate on audit engagements, reviews to a lesser extent, and do not cover other assurance engagements.

4. Section 290 of the Code essentially provides narrative passages pertaining to such matters as financial interests, family and personal relationships, temporary staff assignments and a host of other situations which may threaten independence. In this text we have chosen to illustrate the application of the conceptual approach to these potential independence problems by way of example. We have described a situation, circumstance or relationship, identified the threat posed and then suggested suitable safeguards.

The conceptual approach applied to independence

1. Before considering the conceptual framework approach to independence, we should consider what independence comprises. It comprises:

1.1 ***Independence of mind*** – the state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgement, allowing an individual to act with integrity, objectivity and professional scepticism.

1.2 ***Independence in appearance*** – the avoidance of facts and circumstances that are so significant, a reasonable and informed third party, weighing all the specific facts and circumstances, would reasonably conclude a firm's or a member of the assurance team's integrity or ability to apply objectivity or professional scepticism, had been compromised.

As can be seen from the definitions above, independence is about ***an independent state of mind*** and the ***appearance of independence***. Both are very important. Why? Bear in mind that a member who has, for example, a financial interest in a client may actually perform his duties to that client with the highest level of independence (state of mind) ***but*** will still not be perceived to be independent by any party who is aware that he has a financial interest in the client (appearance). The member should not only "be independent, he should be seen to be independent."

2. As was explained in the introduction to this chapter, the SAICA Code is built on the premise that it is not possible to have a rule for every single ethical issue which may arise; likewise it is impossible to define and list every single situation where a chartered accountant's independence may be threatened. The Code therefore seeks to present chartered accountants with an approach which, if adopted, will provide an appropriate evaluation of, and response to, situations which may threaten independence. As we have seen, this (conceptual) approach requires that chartered accountants in public practice:

2.1 Identify threats to independence.

2.2 Evaluate the significance of the threats identified.

2.3 Where the threats are ***not*** clearly insignificant, apply appropriate safeguards to eliminate or reduce the threat to an acceptable level.

3. Determining whether a threat is "clearly insignificant" is a matter of professional judgement. Every threat is surrounded by different circumstances so there is no ready checklist which can be consulted to measure the significance of a threat. In making the decision the following questions should be addressed:

3.1 Is the overriding requirement to ensure that independence in ***mind*** and ***appearance*** is maintained, under threat?

3.2 Has the extent of public interest been addressed? (Note: the significance of the threat will be increased where there is high public interest in the assurance client e.g. a listed company, a unit trust company).

3.3 What would a reasonable and informed third party, having knowledge of all relevant information, conclude on the significance of the threat?

3.4 Can the threat be regarded as trivial and inconsequential? (clearly insignificant).

Threat: The wife of the partner in charge (engagement partner) of the audit of Cowslip Ltd is appointed as the financial director of Cowslip Ltd.

Insignificant? No. Independence of mind is likely to be threatened and independence in appearance is ***definitely*** threatened, as the husband will be auditing the work of his wife. Even if he acts independently, he will not appear to be independent. There are potential self-interest, intimidation and familiarity threats.

Safeguard: Appoint another partner as engagement partner. Ensure that the former engagement partner does not play any role at all in providing any services to Cowslip Ltd, or resign the engagement.

The conceptual approach also requires that the public interest be considered. It proposes that when ***evaluating the significance*** of any threat, the public interest must be taken into account. As there is considerable public interest in listed companies, pension fund and unit trust companies, any threats to the independence of chartered accountants involved in assurance engagements with such companies, take on additional significance and must be dealt with accordingly. For example, in the illustration given above, if Cowslip Ltd was a large listed company, the appropriate safeguard may be for the firm to resign from the audit engagement or ask the partner to resign from the partnership.

Illustrative examples

The examples laid out in the charts which follow, describe specific situations, circumstances or relationships which may create threats to independence. The charts classify the threat, and indicate which safeguards might be appropriate. Remember the fundamental principle which is primarily under threat is ***objectivity***.

The following definitions are important for this section

1. ***financial interest***:
* an interest in an equity or other security, debenture, loan or other debt instrument of an entity, including rights and obligations to acquire such an interest.

2. ***direct financial interest:***
* a financial interest owned directly by, and under the control of, an individual or entity or
* a financial interest beneficially owned through an investment vehicle, (e.g. unit trust, mutual fund), trust, estate etc, which is ***controlled*** by the individual or entity.

3. ***indirect financial interest:***
* a financial interest beneficially owned through a collective investment vehicle, (e.g. unit trust, mutual fund) estate or trust over which the individual or entity has ***no control.***

4. ***immediate family***:
* spouse (or equivalent) or dependent

5. ***close family:***
* parent, child or sibling who is not an immediate family member.

6. For the purposes of Sec 290 – Independence – Audit and Review Engagements, the terms audit, audit team, audit engagement, audit client and audit report, are deemed to include review, review team, review engagement, review client and review report.

Situation, Circumstance, Relationship	*Threat*	*Safeguards*
1. Financial interests in an audit client		
1.1 A member of the audit team or his ***immediate family member*** (spouse or dependent) ***or the firm*** has a direct or material indirect financial interest in an audit client.	Self-interest	* Disposal of the financial interest if held by the firm or withdrawal from the engagement. * Disposal of the financial interest before the individual becomes a member of the audit team if held by the member of the team or his immediate family member. * Disposal of the indirect financial interest in total or to the extent that it is no longer material before the individual becomes a member of the audit team. * Removal of the member of the audit team from the audit engagement. Note 1: If the financial interest arises out of an inheritance, a gift or as a result of a merger the same threat will exist and the same safeguards can be applied i.e. disposal at the earliest practical date or removal of the member from the audit team. Note 2: ***None*** of the following shall have a direct financial interest or a material indirect financial interest in an audit client • a member of the audit team • an immediate family member of this individual • the firm.
1.2 A ***close family member*** (parent, child, or sibling) of the member of the audit team has a direct or material indirect financial interest in an audit client. Note: the significance of the threat will depend upon * the nature of the relationship between the member of the audit team and the close family member * the materiality of the financial interest to the close family member. * the significance and influence of the member of the audit team in relation to the audit	Self-interest	* Disposal of the interest (or portion thereof) at the earliest date. The close family member will have to make this decision. * Notifying the audit client's governance structures (e.g. the audit committee) of the interest. * providing an additional independent review of the work done by the member of the audit team with the close family relationship. * removal of the affected member from the audit team.

1.3 The firm or a member of the audit team (or a member of his immediate family) holds a direct financial interest or a material indirect financial interest in an audit client ***in the capacity of a trustee***. ***Example.*** Joe Soap and Co, an audit firm, is a trustee of Laduma Trust. Laduma Trust holds shares in Plexcor (Pty) Ltd. Joe Soap and Co are the auditors of Plexcor (Pty) Ltd.	Self-interest	* The firm or member of the audit team should resign the position of trustee. However, resignation will ***not*** be necessary if: • the firm, or the member, or the member's immediate family are ***not beneficiaries*** of the trust • the interest held by the trust in the audit client is ***not material*** • the trust is ***not able to exercise significant influence*** over the audit client and • the firm or the member of the audit team do not have ***significant influence over the investment decisions*** of the trust.
1.4 ***A partner*** in the office of the engagement partner, or his immediate family holds a direct or material indirect financial interest in an audit client.	Self-interest	* the holder of the financial interest must dispose of it as no safeguards can reduce the self-interest threat to an acceptable level * the audit appointment may have to be given up (Note that the immediate family member cannot be forced to dispose of the financial interest).
1.5 Other partners and managerial employees or their immediate family members, hold a direct or material indirect financial interest in an audit client to which they provide ***non-assurance*** services (e.g. IT services).	Self-interest	* if the involvement of partners and managerial employees is anything other than minimal, the holder of the interest must dispose of it.
1.6 An individual who has a ***close personal relationship*** with a member of the audit team, e.g. best friend, has a direct or material indirect financial interest in the audit client.	Self-interest, familiarity	* notifying the audit client's governance structures (e.g. the audit committee) of the interest (in effect obtaining their approval). * providing an additional independent review of the work done by the member of the audit team who has a ***close personal relationship*** with the person who has the financial interest. * removal of the member from the audit team. * excluding the member from significant decision making on the audit.
1.7 A member of the audit team or his immediate family member or the firm has a direct financial interest (or a material indirect financial interest) in an entity which has a controlling interest in the audit client and the client is material to the entity. ***Example.*** Ridabike (Pty) Ltd is 60% owned by Denise Chetty. Ridabike (Pty) Ltd owns 75% of the shares in Roadie (Pty) Ltd. Roadie (Pty) Ltd is audited by Das Chetty. He is Denise Chetty's husband. Roadie (Pty) Ltd is one of Ridabike (Pty) Ltd's major investments.	Self-interest	* the holder of the financial interest must dispose of it or * the audit appointment must be given up (note: Denise Chetty cannot be forced to dispose of her investment so Das Chetty may have to resign the audit appointment).

2. Loans and guarantees		
2.1 A loan or guarantee made by an audit client that is a bank or similar institution, to ***the firm*** under normal lending procedures, terms and requirements.	No threat (The threat arises if the loan was ***not*** made under normal lending conditions)	***Comment***. Some threats, (self interest) could arise if the loan is material to the audit firm. This would be especially significant if the firm is in any way financially dependent on the audit client to the extent that audit decisions could be affected. The only suitable safeguard may be for the audit firm to seek financing from a non-client financial institution.
2.2 A loan by an audit client that is a bank or similar institution made to a ***member of the audit team*** (or his immediate family) under normal lending procedures, terms and requirements. Examples: mortgages, overdrafts, vehicle finance.	No threat (as above)	***Comment***. If the loan was ***not*** made according to normal lending procedures, terms and requirements, it should be thoroughly investigated by the bank, the audit firm and the member of the audit team should be removed from the audit engagement and be required to pay back the loan.
2.3 The firm or a member of the audit team (or immediate family) makes or accepts a loan ***to*** or ***from*** an audit client other than a bank or similar institution or a director or officer of the client. Note: this amounts to direct financial involvement.	Self-interest	* The loan should be cancelled and repaid unless it is immaterial to both parties. There is no other suitable safeguard.
3. Business relationships		
3.1 The firm or a member of the audit team (or immediate family) has a close business relationship with an audit client or its management e.g. • a joint venture • an agreement whereby the firm acts as a distributor or marketer of the audit client's products/services or vice versa (e.g. accounting package software).	Self-interest and intimidation e.g. client threatens to terminate the business relationship if certain audit problems are not overlooked.	* termination of the business relationship. * reducing the magnitude of the relationship so that the financial interest is immaterial and the relationship is clearly insignificant. * resigning the audit engagement. * removing the member from the audit team (i.e. where the close business relationship is between the member of the team and the audit client). * independent review of member of the audit team's work.
3.2 A firm or a member of the audit team purchases goods from an audit client in the normal course of business on an arms length basis.	No threat	***Comment***. Some threat (self-interest, intimidation) may arise if the transactions are • not in the normal course of business or • not arms length (potential intimidation) • of significant nature or magnitude If this is the case, safeguards should be * cancelling or reducing the transactions (including any future transactions) * notifying the clients governance structures (e.g. audit committee) * removing the member from the audit team * firm policy that prohibits audit team members from transacting with an audit client

4. Family and personal relationships		
4.1 An ***immediate*** family member (spouse or dependent) of a member of the audit team is * a director, an officer or an employee (e.g. financial controller) who is in a position to exert direct and significant influence over the subject matter of the audit engagement, at the client.	Self-interest, familiarity and intimidation	* The member must be removed from the audit engagement team. * Possibly restructuring the responsibilities of the audit team so that the member of the audit team does not deal with the immediate/close family member. Note: In terms of Sec 90 of the Companies Act 2008 an individual who is related to any director or employee or consultant who is involved in the maintenance of the company's financial records or preparation of its financial statements may not be appointed auditor (designated auditor).
4.2 A ***close*** family member (parent, child or sibling) of a member of the audit team is a director, an officer or an employee who is in a position to exert direct and significant influence over the subject matter of the audit engagement, at the client. ***Comment***. The likelihood of the threat will have to be assessed in terms of the position the close family member holds with the client, and the role filled by the member of the audit team on the audit.	Self-interest, familiarity and intimidation	* The member of the audit team must be removed from the audit engagement.
Example 1. Zeb Ngidi is a junior trainee on the audit team. His father is the factory manager of the audit client.	Insignificant threat	No safeguard required
Example 2. Raj Naidu is the senior-in-charge of the audit of Megamen (Pty) Ltd. His brother is the financial controller of Megamen (Pty) Ltd, a senior financial position. Note 1:The same principles as discussed under 4.2 will apply to a person other than a close family member who has a close relationship with a member of the audit team e.g. a lifelong friend ***and*** who is a director, officer or employee in a position to exert direct or significant influence over the subject matter of the audit engagement at the client. Note 2:Consideration must be given as to whether a self-interest, familiarity or intimidation threat arises where a personal or family relationship between a partner or employee of the firm ***who is not a member of the audit team*** and a director, officer or employee of the audit client, who is in a position to exert direct influence on the subject matter of the audit engagement	Self-interest, familiarity and intimidation	Safeguards against the threat posed by ***example 2*** would be: * removing Raj Naidu from the audit team * structuring Raj Naidu's responsibilities in such a way that he does not have to deal with matters which are the responsibility of his brother e.g. he is no longer the senior-in-charge of the audit * having any work carried out by Raj Naidu, independently reviewed.

exists. ***Example***. Jacqui Chan, a tax partner of Corbett and Co, an audit firm, has a close personal relationship with Chuck Morris, an employee at Kwando (Pty) Ltd, an audit client. Jacqui Chan is not part of the audit team. Whether or not the threats arise will depend on • the nature and "closeness" of Jacqui Chan and Chuck Morris' relationship. • the extent of influence (if any) Chuck Morris has in the subject matter of Kwando (Pty) Ltd's financial statements. • his seniority in the company.		
5. Employment with an audit client		
5.1 A member of the audit team, or partner of the audit firm, leaves the firm to take up a position as a director, an officer or an employee of the audit client. ***Comment***. The significance of the threat to independence will have to be assessed in terms of the following • the position the former member has taken at the audit client • the amount of involvement the former member of the audit team will have with the audit team • the position the former member held within the audit team • the length of time which has elapsed since the former member was part of the audit team. ***Example 1.*** Art Simon, the former manager in charge of the audit of Crossbow (Pty) Ltd, took up a position as financial controller at Crossbow (Pty) Ltd during the year currently under audit – potentially a high threat to independence. ***Example 2.*** 3 years ago, Geoff Martin joined Crossbow (Pty) Ltd as a credit controller. He had previously worked as a 2nd year trainee on the audit of Crossbow (Pty) Ltd – no threat to independence.	Self interest, familiarity and intimidation	If a threat to independence does exist, the following safeguards should be considered and applied as necessary: * Introducing changes to the audit strategy and audit plan * Assigning a strong and experienced audit team to the engagement (to counter any intimidation threat) * Introducing an additional review (of the audit work) by a partner/manager who was not a member of the audit team.

5.2 A member of the audit team participates in the audit engagement while knowing he will be joining the audit client at some stage in the future. (Note: the member of the audit team may deliberately overlook certain audit "problems" so as not to jeopardise his future employment with the audit client.) Note: If the designated (key) audit partner of a public interest entity audit (e.g. listed company) joins the company as * a director or prescribed officer or * an employee in a position to exert significant influence over the preparation of the client's accounting records or the financial statements on which (his former) firm will express an opinion, a familiarity or intimidation threat will be created and independence would be deemed to be compromised ***unless*** * subsequent to the partner ceasing to be the key audit partner, the public interest entity has issued audited financial statements covering a period of at least 12 months * and the former partner did not work on the audit.	Self-interest (and familiarity)	* Policies and procedures at the firm which require employees to notify the firm when entering serious employment negotiations with an audit client. * Removal of the member from the audit team. * Performing an independent review of any significant judgements made by the member of the audit team while on the engagement.
6. Temporary Staff Assignments		
A firm lends a trainee (or other staff member) to an audit client to assist in the accounting department. Note: A firm employee who has been loaned to an audit client may not take on any management responsibilities at the client. There are no safeguards which could make such a situation acceptable.	Self-review	The following safeguards must be applied * The trainee/employee may not • make any management decisions • exercise discretionary authority to commit the client e.g. sign a purchase order, write off a bad debt. * The trainee on "loan" should not be given ***audit*** responsibility for any function he performed whilst on loan. * The audit client must acknowledge its responsibility for directing and supervising the "on loan trainee". * The loan of the staff member should be for short period only. * The trainee on "loan" does not form part of the audit team.

7. Recent service with an audit client		
7.1 An individual who ***during the period covered by the audit report,*** has been a director, officer, or employee in a position to exert direct and significant influence over the subject matter of the audit engagement, joins the audit firm which conducts the audit of his former company. ***Example.*** Max Mosely CA(SA), resigned from Crafters Ltd where he had been employed as the financial controller for 5 years, half way through the current financial year. He was offered, and accepted the position of audit manager at Uyse and Co, the auditors of Crafters Ltd.	Self interest, familiarity and self-review (may be auditing his own work)	* This individual should ***not*** be assigned to the audit team for that client's audit, as no safeguards can reduce the threat to an acceptable level. Note: In terms of Sec 90 of the Companies Act 2008, a person who was a director at any time during the five financial years preceding the current year, may not be ***appointed*** as auditor. This does not legally prevent the person from working as part of the audit team, but in terms of the Code, he should not. Note: If the individual as described in 7.1, joined the audit firm prior to the period covered by the audit report, the significance of the threat which this situation poses will take into account • the position the individual held with the audit client • the length of time that has passed since the individual left the audit client and • the role the individual fills on the audit team If the threat is perceived to be significant, the following safeguards may be applied * not assigning the individual to the audit team for that client * introducing an additional review of the individual's work on the audit * notifying the client's governance structures of the situation.
8. Serving as an officer or a director of an audit client		
8.1 A partner or employee of the firm accepts an appointment to serve as an officer or director of the audit client (without resigning from the audit firm).	Self-review and self-interest, advocacy (promoting the position of the client)	* The firm ***must*** withdraw (resign) from the audit engagement ***or*** the partner/employee ***must*** resign from the firm. There are no other safeguards which will reduce the threats to an acceptable level. Note: In terms of Sec 90 a director, officer or employee of the company may not be the auditor of the company. Note: In terms of Sec 90, an individual appointed as company secretary may not be appointed auditor.

9. Long association of senior personnel with an audit client		
Senior personnel e.g. partner/manager have been involved with the client over a long period of time. ***Example***. John Jonas, the audit manager of Contion Ltd, has been associated with the client for 10 years, starting as a first year trainee and working his way up to manager on the audit. As he spends many hours at Contion Ltd, he has his own office and is listed in the internal telephone directory.	Familiarity and self-interest	* changing the senior personnel on the audit team on a planned basis * introducing additional independent reviews by a chartered accountant of the work done by the partner/manager * regular internal or external quality control reviews. Note: Sec 92 of the Companies Act 2008 states that the same individual may not serve as the ***designated auditor*** for more than 5 consecutive years. As John Jonas is not the designated auditor, Code safeguards would be applied as indicated above.
10. Provision of non-assurance services to an audit client		
Management responsibility. As a basic principle management is responsible for mmanaging the entity and the auditor should not in any way take over this responsibility whether the company is a public or private company as it presents a significant threat to independence.		
10.1 A firm is requested by an audit client to provide the following ***non***-assurance services: • authorisation, execution and consummation of certain transactions • making certain business decisions for the client • management reporting • setting policy and strategic direction • supervision of the client's staff in the performance of their normal activities • taking responsibility for designing, implementing and maintaining internal control.	Self-interest and self-review and advocacy	* The firm should ***not*** permit the rendering of such non-assurance services to audit clients. This policy must be conveyed to all audit teams and those at the firm involved in formulating the terms of engagement with audit clients. Note 1. All of the services listed under 10.1 are management client responsibilities. Note2. In terms of Sec 94 of the Companies Act 2008, the audit committee of a public company must determine the nature and extent of ***non-audit work*** carried out by the auditor ***and*** must be satisfied that the auditor is and remains independent.
10.2 A firm ***advises*** an audit client on accounting principles and disclosure or the appropriateness of financial and accounting controls or the methods used in determining stated amounts of assets and liabilities or proposed adjusting journal entries.	No threat	These activities are considered to be "part of the dialogue of the audit process" and an appropriate means to promote the fair presentation of the financial statements. The auditor ***advises*** and ***assists***, but does not ***make decisions***.

11. Preparing accounting records and financial statements for an audit client		
The Code draws a distinction between "public/listed companies" and "private companies". It states that a firm should not provide accounting and bookkeeping services (as listed below) to a public/listed company which is its audit client. However it suggests that the firm may provide the services listed below to a private company which is its audit client provided the appropriate safeguards are put in place to reduce any self-review threat to an acceptable level. 11.1 A firm provides the following accounting and bookkeeping services to an audit client. • recording transactions which the client has approved and classified • posting such transactions to the client's general ledger • posting client approved entries to the trial balance. • preparing the client's payroll and related services e.g. submitting PAYE returns • drawing up the annual financial statements from the trial balance ***Comment***. There appear to be two issues here. Firstly, are the services described above part of the preparation of the financial statements (which is a management responsibility) and secondly, are the services considered to be part of "habitually or regularly performing the duties of accountant or bookkeeper…" because in terms of Sec 90 of the Companies Act 2008, a person who performs the duties of accountant or bookkeeper may ***not*** be appointed as auditor (because of the obvious lack of independence). Traditionally the services listed above have ***not*** been regarded as "habitually or regularly performing the duties of accountant or bookkeeper" so Section 90 of the Companies Act would not apply. However, a self-review threat still arises and safeguards should be put in place.	Self-review	In the case of ***public*** companies, the best safeguard would be compliance with the audit committee's interpretation of accounting and bookkeeping services. The audit committee * must approve all non-audit work and * must be satisfied that the auditor is independent. In the case of a ***private*** company, if the audit firm perceives that a significant threat may arise, safeguards might include * arranging for such services to be performed by someone ***not*** on the audit team * notifying the audit team that they may ***not*** make any ***management decisions.*** * clarifying for management • that management is responsible for source data, transaction approval, journal entry origination and approval etc. • what the audit team is permitted to do. Note: In the situation where a company avoids an audit and qualifies to have its AFS independently reviewed because the AFS are externally compiled, ***the reviewer*** (who will frequently be a chartered accountant) may not also be ***the compiler*** of the AFS (lack of independence).

12. Valuation services		
A firm performs a valuation (of an asset, liability, investment) for an audit client which is to be incorporated into, or used in conjunction with, the client's financial statements. ***Example***. Company A holds 20% of the shares in (private) company B. The directors of A request the auditors to value the investment at reporting date, so that the fair value can be incorporated into the year-end financial statements. Note again that in the case of a public company the audit committee must determine the nature and extent of any non-audit work to be conducted by the auditor. This is an effective safeguard.	Self-review	Where the valuation has a material effect on the financial statements and involves a significant degree of subjectivity the valuation service should ***not*** be undertaken. Where a valuation service is undertaken, the self-review threat could be reduced to an acceptable level by the introduction of the following safeguards * Ensuring that the personnel who perform the valuation, are not part of the audit team. * Involving an individual who was ***not*** a member of the audit team to ***review*** the valuation. * Confirming with the client, its understanding of the underlying assumptions and methodologies used in the valuation and obtaining its approval thereof.
13. Provision of taxation services to an audit client		
Taxation services can be broken down into four broad categories, each of which may present different kinds of threat or no threat at all. The four categories are * preparation of tax returns * carrying out tax calculations for the purpose of preparing accounting entries * tax planning and advisory services * assistance with resolution of tax disputes.		
13.1 The audit firm assists with the preparation of tax returns and advises the audit client on any queries arising from the SARS relating to the tax return.	No threat	Taxation services are generally not perceived to impair independence ***but*** the audit firm must be careful not to make management decisions or assume responsibility for the tax affairs of the audit client. The role should be advisory.
13.2 The firm prepares calculations of current and deferred tax liabilities for the purposes of preparing journal entries for a ***private*** company which will be subsequently audited.	Self-review	Safeguards could include: * Using individuals who are not members of the audit team to perform the service. * Using a partner who is not a member of the audit team to ***review*** the calculations. * Not performing the service if the calculations have a very material effect on the financial statements. * Obtaining advice from an external tax professional. * Complying with the audit committees ruling on non-audit work.

13.3 As in 13.2 above but for ***public/listed*** companies.		* The Code states that the auditor should ***not*** prepare tax calculations for a public company that are material to the financial statements other than in an "emergency"
13.4 The firm provides tax planning and advisory services which will affect matters to be reflected in the financial statements.	Self-review	Safeguards as above. Note: If the advice given is clearly supported by the tax authority, precedent or established practice, then generally speaking no threat to independence arises.
13.5 The firm represents an audit client in the resolution of a tax dispute, which has arisen from SARS rejecting the client's arguments on a particular issue and the matter has been referred to a hearing/court by either the SARS or the audit client.	Self-review or advocacy.	* Safeguards as above. However, if the amounts involved are material to the financial statements on which the auditor will express an opinion, there are ***no*** safeguards which would reduce the threat posed (by acting for the client) to an acceptable level.
Comment. Chartered accountants who render professional tax services in any form may often find themselves faced with difficult situations. Generally clients do not like paying tax and may go to great lengths to evade tax. Clients may request a chartered accountant to submit false returns on their behalf, or may themselves deliberately withhold information from the chartered accountant who is acting on their behalf so as to evade tax. Some clients may even become abusive with a chartered accountant or make claims that "Everyone evades tax, so why shouldn't I?" Paying tax can be an emotive issue but the overriding requirement is that a chartered accountant should not be associated with any taxation return or communication in which there is reason to believe that it: * contains a false or misleading statement * contains statements or information furnished recklessly or without any real knowledge of whether they are true or false * omits or obscures information required to be submitted and such omission or obscurity would mislead the revenue authorities. To assist a client to ***evade*** tax will amount to a failure to comply with the fundamental principles.	Objectivity, integrity and professional behaviour.	The following safeguards should protect the chartered accountant: * A chartered accountant should put forward the best position in favour of a client, provided he does so: • with professional competence, integrity and objectivity, • within the bounds of the law. * A chartered accountant should ensure that the client understands that: • tax services and advice offered may be challenged by the South African Revenue Services where they are based on opinion rather than fact, as is often the case, • responsibility for the ***content*** of a tax return rests with the client even where the return has been prepared by the chartered accountant. * Material matters relating to tax advice/opinions given to a client, should be recorded in writing. This is essential to prevent a client accused of tax evasion, from falsely claiming that he was "following the advice given to him by the chartered accountant". * In preparing a tax return, a chartered accountant may rely on information furnished by the client, provided : • the information appears reasonable, • the chartered accountant makes use of the client's returns for prior years where feasible,

		• the chartered accountant makes reasonable enquiries when information appears incorrect or incomplete ***but*** the chartered accountant is encouraged to: • request supporting data as required, • make reference to relevant documents and records of the client's business operations. * Where a chartered accountant discovers that there have been material errors or omissions relating to tax returns submitted in respect of prior years, he should: • notify the client of the error or omission • advise the client to make full disclosure of the error or omission to the revenue authorities • advise the client of the powers of the revenue authorities to obtain information which they may require e.g. seize the client's books and records and to impose penalties, e.g. double the amount of tax payable. ***Comment.*** It is quite possible that the client was well aware of the omission and is not prepared to make any disclosures. This creates a difficult situation for the chartered accountant if he is associated with the incorrect return which was submitted. In terms of the fundamental principle of confidentiality, the chartered accountant may not inform, at this stage, the revenue authorities without permission, as this may be a breach of confidentiality; on the other hand Section 110 of the Code, states that a member should not be associated with any false return. Advice given by the technical department of SAICA on this anomaly in the Code is that a chartered accountant who is associated with a false return which has been submitted, and which the client will not rectify, should notify the revenue authorities that his association with the return can no longer be relied upon ***but*** without giving any details. Legal advice should be taken before doing this! Of course this action will alert the authorities to the problem and they will follow it up. * As a general rule a chartered accountant should not continue an association with a dishonest client, and should be aware that in terms of Section 105 of the Income Tax Act, the Commissioner is empowered to report a chartered accountant to SAICA for unprofessional conduct.

14. Provision of internal audit services to an audit client		
Internal audit functions vary and can include * monitoring of internal controls * reviewing the economy, efficiency and effectiveness of operating activities, both financial and non-financial * assessing risks faced by the company and the company's responses thereto * reviewing compliance with laws and regulations, management policies etc. All of the above are responsibilities of management so if the external auditor gets too involved with these activities there is a significant threat that the auditor will be assuming management responsibilities, which is not acceptable as it will compromise the auditor's independence. Furthermore, if the firm uses the work of internal audit in the course of the external audit, there is a potential self-review threat to independence.		
14.1 providing internal audit services such as the following would equate to assuming management responsibilities * setting internal policy and strategic direction for internal audit * directing and taking responsibility for internal audit's employees * deciding which recommendations from internal audit should be implemented * performing procedures such as business risk assessment on behalf of internal audit.	Self-review	* Although not specifically prohibited by the Companies Act 2008, the provision of both internal and external audit services by the same firm is unlikely to be acceptable to the audit committee for independence reasons. It would also be contrary to the King III Report on Corporate Governance, particularly for public (listed) companies. * The best safeguard would therefore be not to offer both internal and external audit services to the same client. However, the Code does state that a firm can offer (some) internal audit services and at the same time avoid assuming management responsibility if management • designates an appropriate and competent resource to be responsible at all times for internal audit activities and to acknowledge responsibility for designing, implementing and maintaining internal control. • reviews, assesses and approves internal audit work (scope, risk and frequency). • evaluates the adequacy of the internal audit services and findings and determines which recommendations to implement. • reports to those charged with governance on the significant findings and recommendations arising from the internal audit service. * In the case of a public company the audit committee would have to approve the appointment to do this work.
e.g. Note: In some situations there may be internal audit work which the audit firm can do which presents no threat, for example where the audit firm provides internal audit services of an operational (not financial) nature, e.g. an evaluation of an audit client's product distribution system.		

15. Provision of Information Technology services to an audit client		
15.1 The audit firm provides design and implementation services for financial systems which form a significant part of the internal control over financial reporting or which are used to generate information which forms part of a client's financial statements e.g. revenue and receipts cycle software. Note: The following IT systems services are deemed ***not*** to create a threat to independence (as long as the firm's personnel do not assume a management responsibility) for either a private or public/listed company. * design and implementation of IT systems unrelated to internal control over financial reporting or which do not generate information forming a significant part of the accounting records e.g. a sales forecasting system. * implementing "off the shelf" accounting or financial reporting software (not developed by the firm) * evaluating and making recommendations with respect to a system designed, implemented or operated by another service provider.	Self-review	If the audit client is a ***public/listed*** company the audit firm should ***not*** provide IT services as described under 15.1 as no safeguards can reduce the threat to independence to an acceptable level (because of the level of ″public interest″ in the audit client). If the audit client is a ***private*** company the safeguards to address the threat should include the following * The audit client acknowledges its responsibility for establishing and monitoring a system of internal controls. * The audit client designates a competent, senior employee with the responsibility of making all management decisions with respect to the design and implementation of the hardware or software required. * The audit client evaluates the adequacy and results of the design and implementation of the system, and * The audit client is responsible for the operation of the system (hardware and software) and the data used or generated by the system. * The IT service is carried out by personnel ***not*** involved in the audit engagement.
16. Provision of litigation support services to an audit client		
Litigation support services include acting as an expert witness, calculating estimated legal damages payable or receivable, or assisting in gathering documentation in relation to a dispute/litigation. A self review threat will usually arise only where the result of providing the litigation service affects the financial statements e.g. where the service involves assisting with determining an estimate of legal damages which must be disclosed in the financial statements.	Self-review	Safeguards might include: * Using professionals (from the firm) who are ***not*** members of the audit team to perform the service * Using independent experts * Ensuring that the firm does not make management decisions on behalf of the client.
17. Provision of legal services to an audit client		
Legal services differ from litigation support services. ***Legal services*** are defined as services which can only be offered by a qualified lawyer. (Many of the larger firms employ lawyers.) ***Litigation support services*** (see 16 above) can be provided by anyone with the necessary expertise.		

17.1 The legal service provided supports an audit client in the execution of a transaction e.g. drafting a contract, providing legal advice, or providing legal due diligence for say, a merger.	Self-review	If the following safeguards are put in place, the threat would normally be insignificant * the lawyer who provides the legal service is not a member of the audit team. * having a lawyer who was not involved in providing the legal service, • advise the audit team on the details of the service and • performing a review of any treatment of matters arising from the legal service in the financial statements.
17.2 The legal service provided is to act for an audit client in a dispute or litigation when the amounts involved are ***material in relation to the financial statements*** on which the firm will express an opinion.	Self-review and advocacy	This legal service should ***not*** be undertaken by an audit firm on behalf of an audit client.
17.3 The legal service provided is to act for an audit client in a dispute or litigation when the amounts involved are ***not material in relation to the financial statements*** on which the firm will express an opinion.	Normally no threat	If the audit firm is concerned that there may be an advocacy or self review threat the safeguards described under 17.1 could be applied to reduce the threat to an acceptable level.
17.4 The audit client wishes to appoint a partner or employee of the firm which holds the audit appointment as legal advisor i.e. the person to whom legal affairs are referred. (The person appointed remains an employee of the audit firm). Note: a partner in an audit practice may, besides being a registered auditor, also be a qualified lawyer.	Self-review and advocacy	A partner or employee of the audit firm should ***not*** accept this appointment (A legal advisor is generally a senior management position, and independence would be significantly threatened.)
18. Recruiting senior management on behalf of an audit client		
18.1 The firm is engaged to recruit suitable accounting staff for an audit client.	Self-interest, familiarity	Safeguards should include the following * Limiting the service to reviewing the suitability of applicants against a list of criteria drawn up by the client * Leaving the final decision to the client * Ensuring that the service is rendered by a professional at the firm who is not a member of the audit team.
18.2 The firm is engaged by a public/listed company which is an audit client to recruit a senior employee who will be in a position to exert significant influence over the preparation of the client's accounting records or the financial statements on which the firm will express an opinion e.g. the financial director.	Self-interest, familiarity	In addition to the above, where the audit client is a public/listed company, the following additional safeguards should be implemented. The audit firm should not: * Search for candidates to fill such positions as described in 18.2 * Undertake reference checks of prospective candidates for such positions as described in 18.2.

19. Corporate finance services		
Whether providing corporate finance services will threaten independence, will depend upon the nature of the service. ***Examples*** 19.1 The firm promotes, deals in, or underwrites an audit client's shares	Self-interest and advocacy	These activities should ***not*** be undertaken by the audit firm as there are no safeguards which would reduce the threat to an acceptable level.
19.2 The firm assists an audit client in developing corporate finance strategies and/or introduces clients to sources of finance and/or identifies potential targets for the audit client to acquire. Note: Providing some types of corporate finance services may materially affect the amounts reported in the financial statements on which the firm will express an opinion. Self-review threats may arise.	Self-interest, self-review and advocacy threats.	Safeguards which could be applied * Ensuring that management decisions are not made on behalf of the client by implementing a client approval procedure as the assignment progresses * Using individuals from the firm who are not members of the audit team on corporate finance assignments. * Having an individual who was not involved in the corporate finance service • advise the audit team on the details of the service and • review any accounting treatment for transactions arising from the corporate finance service * Ensuring that the firm does not commit the client to anything or consummate a transaction on behalf of the client * Discussing the engagement with the governance structures of the client. * Disclosing to the client any financial interest which the audit firm may have in the advice it renders e.g. the firm receives a commission from the source of finance it introduces to the audit client.
20. Fees		
20.1 ***Fees – relative size*** The fees generated by one audit client represent a large portion of a firm's total fee income. Note: the audit firm may compromise its independence because they do not want to lose the client (self-interest). There is also a possibility that the client, realising that the audit firm derives a large proportion of its income from it, will put pressure on the audit firm by threatening to end the relationship (intimidation).	Self-interest, intimidation	Safeguards should include the following * Discussing the matter with the clients governance structures * Taking steps to reduce dependency e.g. actively seeking new clients * Introducing external quality control reviews * Consulting a third party on key audit judgements, e.g. the appropriateness of the audit opinion to be given.

Note: ***"Pre" and "Post" issuance quality control reviews.*** 1. In a situation where an audit client is a public/listed entity and, ***for two consecutive years***, the total fees from the client and its related entities (e.g. an entity over which the client has direct or indirect control such as a subsidiary) represent more than 15% of the total fees received by the audit firm, the firm must: * notify those charged with governance (including the audit committee), of the 15% situation ***and*** must * discuss which of the safeguards described below, the firm will implement to reduce any threats to an acceptable level. ***Safeguard 1***. ***Pre-issuance*** quality control review. ***Prior*** to issuing the audit opinion on the second year's financial statements, a chartered accountant (in public practice) who is ***not*** a member of the firm performs a quality control audit engagement ***or*** ***Safeguard 2. Post-issuance*** quality control review. After the audit opinion on the second year's financial statements has been issued, and before the audit opinion on the third year's financial statements have been issued, a chartered accountant (in public practice) who is ***not*** a member of the firm, performs a quality control review on the second year's audit. 2. The disclosure to, and discussion with, those charged with governance, shall occur each year for as long as the 15% situation continues and one of the two safeguards described above must be applied. 3. If the total fees significantly exceed 15% of the audit, the firm must determine whether a post issuance review will reduce the threat to an acceptable level and if not, a pre-issuance review must be conducted. 4. Note that the quality control review could also be carried out by the IRBA.		
20.2 ***Fees – overdue*** An audit client has not paid its fees for professional services for a long time. Note: This may result in the audit firm not putting the necessary	Self-interest	Safeguards should include the following * Discussing the outstanding fees with the governance structures of the client, e.g. audit committee. * Introducing an additional independent review of the work performed (for quality). However, this will increase the fee!

resources and time into the current engagement, because the partner/manager does not expect the fee to be paid. This threatens independence. 20.3 ***Fees - contingent*** Contingent fees are fees calculated on a predetermined basis relating to the outcome of the work preformed or as a result of a transaction which arises from the service. Note: fees are not regarded as contingent if they are established by a court or public authority e.g. liquidator's fee.		
* A contingent fee is proposed for an audit engagement. The audit firm is required to express an opinion on a set of financial statements which are to be used by the client to support a loan application. The audit client offers to pay a fee equal to 5% of the loan applied for if the application is successful.	Self-interest	A firm may ***not*** enter into a contingent fee arrangement for an audit engagement as no safeguards would reduce the threat to an acceptable level.
* A contingent fee is proposed for a ***non-assurance*** engagement to be rendered to an audit client e.g. the client engages the audit firm to recruit senior personnel. The fee will be an amount equal to 10% of the annual remuneration package payable to the person appointed.	Self-interest	Safeguards which could be implemented include * Disclosing the nature and extent of the fee to the audit client's governance structures prior to the engagement * Having the "fairness" of the fee reviewed or decided upon by an independent third party. * (see also 18 above relating to recruiting).
21. Compensation and evaluation policies		
21.1 Members of the audit team are given a financial bonus for selling non-audit services to the audit client. (The audit team member could be more interested in, or focused on, trying to earn bonuses than on audit work.)	Self-interest	Safeguards could include: * changing or eliminating compensation methods of this nature. * removing the audit team member who sold the non-audit services from the audit team. * having the work of audit team member independently reviewed. Note: An audit partner should not be remunerated based on his success at selling non-assurance services.

22. Gifts and hospitality		
22.1 An audit client wishes to "reward" the firm's audit manager by giving him a holiday trip to America.	Self-interest, familiarity and intimidation	A firm or member of the audit team should ***not accept*** gifts or hospitality which are anything other than clearly insignificant.
22.2 An audit client gives each member of the engagement team an inexpensive pen bearing the company's logo, at the completion of the annual audit.	No threat	In determining whether the gift or hospitality is insignificant, the monetary value should be considered as well as whether the degree of independence in the relationship between the client and audit team will be altered, e.g. has a "professional" relationship become one of "familiarity".
23. Actual or threatened litigation between the firm and an audit client		
Where a client and firm are involved in actual or threatened litigation instigated by either party, the relationship between them is likely to be altered significantly. Both parties are likely to be on the defensive and unco-operative as they have been placed in adversarial positions.	Self-interest or intimidation	As this situation will very often make it impossible for the auditor to perform to the required standards, withdrawal from the audit engagement would normally be the only option. Discussion with the audit committee may resolve the issue.

PART C - CHARTERED ACCOUNTANTS IN BUSINESS

SECTION 300 – INTRODUCTION

1. General

1.1 The majority of chartered accountants work in business. They may be inter alia, salaried employees, a company director, an owner manager. Numerous groupings of individuals, such as investors, creditors, employers as well as the government (e.g. SARS) and the public at large (e.g. ordinary investors in unit trusts) rely on chartered accountants directly or indirectly. This is particularly so where the chartered accountant is involved in the preparation and reporting of financial and other information, but is not restricted to this; chartered accountants are frequently involved in providing financial management and other advice on business matters.

1.2 Chartered accountants in business are expected to encourage an ethics based culture within their organizations. At the same time they themselves have an obligation to comply with the fundamental principles of integrity, objectivity, confidentiality, professional competence and due care and professional behaviour. A simple example to illustrate: A chartered accountant working for a listed company who gets involved in a financial fraud betrays the trust of his employers, investors and fellow employees and discredits the accounting profession.

2. The conceptual framework

2.1 The conceptual framework to be applied by chartered accountants in business is the same as has been discussed for chartered accountants in public practice, that is:

* identify threats to compliance with the fundamental principles
* evaluate whether these threats are clearly insignificant and
* where they are ***not*** clearly insignificant, apply appropriate safeguards to eliminate or reduce the threat to an acceptable level.

3. Threats

3.1 The categorisation of threats for chartered accountants in business remains the same as for chartered accountants in public practice, i.e. self-interest, self-review, advocacy, familiarity and intimidation:

* ***self-interest*** threats are created when a financial or other interest will inappropriately affect the chartered accountant's judgement or behaviour.

Example 1. Lucas Borak, the financial director of Company A has shares in Company A. The financial decisions he makes may be influenced by the effect the decisions will have on his share value and not the facts relating to the decision.

Example 2. Carl Marks, the financial controller at Company B participates in a performance bonus scheme for managers. Financial decisions which Carl Marks makes can materially affect the bonus he receives.

* ***self-review threats*** are created when a chartered accountant in business evaluates a previous judgement or service which he himself has performed. The threat is that the evaluation may be inappropriate, e.g. not diligently carried out.

Example 3. Jackie Jones, the financial director of Company X determines the appropriate accounting treatment for a complex financing transaction which he constructed and approved.

* ***an advocacy threat*** is created when a chartered accountant in business promotes his employer's position to the extent that his objectivity is compromised.

Example 4. In attempting to sell a financial product marketed by the company for which he works Dickie Dell, a chartered accountant, makes use of questionable tactics and debatable statistics in "proving" the superiority of his company's products. (This is an advocacy threat to his integrity, objectivity and professional behaviour.)

* ***a familiarity threat*** is created when a chartered accountant in business will be or become too sympathetic to the interests of some other party because he has a long or close relationship with that party.

Example 5. Billy Alviro, the managing director of Company Z regularly accepts expensive gifts and travel opportunities from two of his company's major suppliers. The threat is that preferential treatment will be given to these two suppliers because they are friends and not because they are the best suppliers for the company. This is a threat to Billy Alviro's objectivity and possibly, his professional competence and due care.

* ***intimidation threats*** are created when a chartered accountant will be deterred from acting objectively because of actual or perceived pressures.

As a chartered accountant in business very often depends upon his employing organization for his livelihood, he can often be placed in a very difficult position where ethical situations arise. He may be put under pressure to act or behave in ways which could threaten his compliance with all of the fundamental principles. A chartered accountant in business may be put under pressure (intimidated by fear of losing his job) to

Example 6. Act contrary to law or regulation, e.g. claim VAT deductions to which the company is not entitled (integrity, professional behaviour, objectivity).

Example 7. Facilitate unethical or illegal earnings strategies, e.g. provide false documentation to conceal the purchase and sale of illegal products (integrity, professional behaviour, objectivity).

Example 8. Lie to, or intentionally mislead (including by remaining silent) others in particular,
- the auditors e.g. produce false evidence to support fictitious sales
- regulators e.g. lie to custom officials about the nature of imported goods to reduce import charges (integrity, professional behaviour, objectivity).

4. Safeguards

4.1 Although the chartered accountant in business will have safeguards created by the profession, legislation or regulation available to him, it is likely that safeguards in the chartered accountant's workplace will be more accessible and relevant to him. For example, a chartered accountant whose compliance with the fundamental principle of professional behaviour is being threatened by intimidation from a superior should have a means of exposing the intimidation (and preventing his non-compliance) without fear of retribution e.g. this may be an individual at the employer appointed to deal with such matters and to whom the chartered accountant can notify of the intimidation. Workplace safeguards may include

* the employer's system of corporate oversight which, inter alia, monitors the ethical behaviour at all levels of management including executive directors.
* strong internal controls, e.g. clear division of duties and reporting lines which hold employees accountable for their actions.
* appropriate disciplinary processes which would strongly dissuade an employee from engaging in unethical behaviour.
* policies and procedures to implement and monitor the quality of employee performance.
* policies and procedures to empower employees to communicate to senior levels any ethical issues without fear of retribution.

4.2 In considering safeguards it must be assumed that the chartered accountant is an ***unwilling*** party to the unethical behaviour. Therefore there should be safeguards that protect the

chartered accountant from any negative effects of doing the "right thing". For example, if pressure is placed on the chartered accountant to lie, he must have a safeguard to turn to

4.3 If a chartered accountant is willing to be party to unethical behaviour which ignores compliance with the fundamental principles, he will have little interest in safeguards, other than how to get around any that may have been implemented by the employer organization. There will also be many situations where only the chartered accountant himself will be aware that he is faced by an ethical situation. For example, he may easily be able to benefit form confidential information which he has without anyone knowing. The appropriate handling of ethical situations will frequently depend on the integrity of the chartered accountant himself.

CONFLICTS OF INTEREST – SECTION 310

1. ***Responsibility***

1.1 A chartered accountant in business shall not allow a conflict of interest to compromise his professional or business judgement. A conflict of interest may arise when

* the chartered accountant undertakes a professional activity (an activity requiring accountancy or related skills) related to a particular matter for two or more parties whose interests with respect to that matter, are in conflict; or
* the interests of the chartered accountant with respect to a particular matter and the interests of a party (e.g. his employer) for whom the chartered accountant undertakes a professional activity related to that matter, are in conflict.

1.2 When identifying and evaluating the interests and relationships that might create a conflict of interest, and implementing safeguards, a chartered accountant in business shall exercise professional judgement and be alert to all interests and relationships that a reasonable and informed third party, weighing all the specific facts and circumstances available to the chartered accountant at the time, would be likely to conclude might compromise compliance with the fundamental principles.

2. Threats

2.1 Primarily a conflict of interest creates a threat to objectivity but may also create a threat to other fundamental principles.

2.2 Situations in which conflicts may arise

Example 1. Shoab Aktar is a chartered accountant in business. He sits on the board of two unrelated companies (A and B) who operate in the same business sector. At a board meeting of company A, Shoab Aktar obtains confidential information that he could use to the advantage of company B, but which would be to the disadvantage of company A. This situation (conflict) creates a threat to his objectivity, confidentiality and professional behaviour and integrity.

Example 2. Tom Collins a chartered accountant in business, has been engaged to provide financial advice to each of two parties to assist them in dissolving their medical partnership. There are a number of contentious issues in the dissolution. This situation could create threats to Tom Collins objectivity, (he may favour one partner over the other), professional behaviour, (he may act in a manner that discredits the profession by favouring one partner because there is some kind of reward for doing so) as well as his integrity.

Example 3. Paul Premium is a chartered accountant employed by company Z. He is responsible for contracting a company to supply a full range of IT support for company Z. Awarding the contract to one of the strong contenders for the contract could result in a financial benefit for an immediate family member (his wife or a dependent). This creates a significant threat to his objectivity and possibly, confidentiality and professional behaviour (if for example he gave the immediate family member confidential information about how they should charge for their services to win the contract).

Example 4. Fred Bennett a chartered accountant in business, sits on the investment committee of company Q. The investment committee approves all major investments the company makes. If the investment committee approves a specific investment, it will increase the value of Fred Bennett's personal investment portfolio. This creates a threat to his objectivity, i.e. Fred Bennett votes to approve the investment, not because it is a good investment for the company, but because it is a good investment for him.

3. Safeguards

To counter the threats arising from a conflict of interest situation the following safeguards may be implemented by the chartered accountant

* disclosing the potential conflict of interest to all parties involved, including the possible consequences of the chartered accountant being conflicted (example 1, 2, 3 and 4)
* obtaining appropriate oversight for the service he has provided, e.g. acting under the supervision of an independent director (example 2 and 3)
* withdrawing from the decision making or authorising processes relating to the matter giving rise to the conflict (example 1, 3 and 4).
* consulting with third parties such as SAICA, legal counsel or other chartered accountants on how to resolve the conflict.

SECTION 320 – PREPARATION AND REPORTING OF INFORMATION

1. Responsibility

A chartered accountant in business who is involved with the preparation and reporting of information that may be used by the public or others, both inside or outside the employing organization, has a responsibility to present such information fairly, honestly and in accordance with the relevant standards, e.g. financial statements should comply with the international financial reporting standards. The same requirements of fair presentation, honesty etc would apply to a management representation prepared for the external auditors by a chartered accountant in business.

2. Threats

Intimidation or self-interest threats to objectively, integrity or professional competence are created where a chartered accountant is pressured by internal or external parties, or by the prospect of personal gain, to prepare or report information in a misleading way or to become associated with misleading information through the actions of others e.g. manipulating reported profits or knowingly benefiting from reported profits manipulated by others, to earn additional bonuses.

3. Safeguards

3.1 To counter an intimidation threat, the chartered accountant may need to make use of safeguards included in those listed under Section 300. Self interest threats can really only be addressed by chartered accountants in business putting preventative measures in place to ensure that they cannot be accused of looking after their own interests. Certain of the safeguards included under Section 310 may be suitable. Of course addressing a self-interest threat requires a willingness on the part of the chartered accountant to comply with the fundamental principles. The chartered accountant shall be particularly alert to threats to the principle of integrity which requires that the chartered accountant be straightforward and honest.

3.2 Where it is not possible to reduce the threat to an acceptable level a chartered accountant in business shall refuse to be or remain associated with information he deems to be misleading and shall take steps to dissociate himself from such information, but without non-compliance with the fundamental principle of confidentiality.

SECTION 330 - ACTING WITH SUFFICIENT EXPERTISE

1. Responsibility

The chartered accountant in business has a responsibility to undertake only those tasks for which he has the necessary training or expertise. If the chartered accountant does not have the necessary expertise he has a responsibility to obtain it.

2. Threats

2.1 The primary threat in this situation is that the chartered accountant may fail to comply with the fundamental principle of professional competence and due care.

2.2 A further threat is that the chartered accountant may intentionally mislead an employer as to the level of expertise or experience he possesses. This would be a self-interest threat to the chartered accountant's objectivity, integrity, professional behaviour and professional competence (he does not have the required experience).

3. Safeguards

The relevant safeguards may be to

3.1 Obtain additional training or seek advice from

- supervisors within the organization
- independent experts
- a relevant professional body.

3.2 Carefully consider the expertise required for the task and realistically assess whether he has the necessary competence and if not, to inform the party to whom he reports of his lack of expertise.

3.3 Ensure that there is sufficient time and the necessary resources to perform the task to the required professional standard.

SECTION 340 - FINANCIAL INTERESTS, COMPENSATION AND INCENTIVES LINKED TO FINANCIAL REPORTING AND DECISION MAKING

1. Responsibility

Where a chartered accountant in business (or his immediate or close family members) has a financial interest in the employing organization, including those arising from compensation or incentive arrangements, he must ensure that he complies with the fundamental principles. A chartered accountant in business shall neither manipulate information nor use confidential information for personal gain, as this will amount to self-interest threats to his compliance with the fundamental principles of objectivity, confidentiality and integrity.

2. Threats

Self interest threats to objectivity, integrity or confidentiality and, at times, professional behaviour may be created. Such threats may arise where the chartered accountant or an immediate or close family member

2.1 Holds a direct or indirect financial interest in the employing organization and the value of the interest can be directly influenced by decisions made by the chartered accountant.

2.2 Is eligible for a profit related bonus and the value of the bonus could be directly affected by decisions made by the chartered accountant.

2.3 Holds share options in the employing organization, the value of which could be directly affected by decisions made by the chartered accountant.

2.4 Engages in insider trading (use of price sensitive confidential information to trade shares) or similar illegal activities.

2.5 The chartered accountant participates in compensation arrangements which provide incentives to achieve performance targets, the amount of which can be influenced by the decisions taken by the chartered accountant.

Note that self-interest threats arising from compensation or incentive arrangements may be further compounded by pressure from superiors or peers whose ″bonuses″ may be influenced by decisions taken by the chartered accountant in business. Example: All management above a certain level at company P participate in a bonus scheme based on the net profit before tax. Peter Pinarello, the chief financial officer and a chartered accountant makes a number of decisions that can affect the reported net profit before tax. As Peter Pinarello is on a management level which will benefit from the ″bonus″ scheme a self-interest threat is created. Pressure from other management on Peter Pinarello to make financial reporting decisions which will maximise net profit before tax (and hence their bonuses) will intensify the self-interest threat and may amount to an intimidation threat.

3. Safeguards

Whether safeguards need to be applied will depend upon the significance of the threat and may include

3.1 A policy which requires all employees to disclose to the company on a regular basis, any financial interest in the company (including the financial interests of close and immediate family).

3.2 A remuneration committee to determine remuneration and any incentive schemes for senior management,

3.3 Internal and external audit procedures to review critical decisions made by the chartered accountant which may affect, for example, bonuses paid.

3.4 Communication of the legal position and consequences of insider trading and similar acts to employees on a regular basis.

3.5 A policy which requires employees to notify a specific individual/committee of any intention to trade in shares of the company.

SECTION 350 – INDUCEMENTS

Receiving Offers

1. Responsibility

The chartered accountant in business (or an immediate or close family member) may be offered a gift, hospitality, preferential treatment etc, in an attempt to unduly influence his actions or decisions or encourage him to act in an illegal or dishonest manner or to reveal confidential information. The chartered accountant has a responsibility to be alert to threats to his compliance with the fundamental principles and ***not*** be influenced by the inducement.

2. Threats

Self-interest threats to objectivity and confidentiality are created. Intimidation threats to objectivity, confidentiality, integrity and professional behaviour may follow if the inducement is accepted; i.e. the provider of the inducement may threaten to make the inducement public (blackmail).

3. Safeguards

To protect against these threats, the chartered accountant in business should

3.1 On receiving the inducement, immediately inform his superior or the company's governance structures.

3.2 Inform third parties of the inducement e.g. the employer of the individual who made the offer (if applicable) but ***not*** before seeking legal advice.

3.3 Inform his supervisor of potential sources of inducements e.g. where immediate family members are employed by competitors or potential suppliers. ***Example:*** The competitor or supplier may offer to promote the immediate family member of the chartered accountant, in return for confidential information or some other favour from the chartered accountant. Advising a supervisor of the potential source of an inducement may not prevent the inducement from being made by the competitor or supplier but at least the chartered accountant's company will be aware of it and could address it accordingly. The chartered accountant has also safeguarded himself against allegations of unprofessional behaviour.

Making offers

1. Responsibility

A chartered accountant in business should not offer an inducement to improperly influence the judgement or behaviour of a third party. Pressure to do so may be placed on the chartered accountant by internal sources e.g. a superior, or from external sources e.g. a business associate who promises a business deal in return for the chartered accountant's company paying for an overseas holiday for the business associate.

2. Threats

Making such offers would threaten the chartered accountant's compliance with the fundamental principles of integrity, objectivity and professional behaviour.

3. Safeguards

3.1 A company policy which prohibits employees (including senior management) from offering an inducement combined with an efficient disciplinary process.

3.2 A procedure which enables the chartered accountant to report to the company's governance structures, any attempts both internal and external, to pressure him into offering inducements.

RULES REGARDING IMPROPER CONDUCT (IRBA)

As you are primarily studying auditing, you should be aware that the IRBA has a set of "rules regarding improper conduct". The opposite of "professional conduct" is "improper conduct" and registered auditors (the majority of whom are also chartered accountants in public practice), if found guilty of improper conduct, may be sentenced to:

* a caution or reprimand
* a fine
* a suspension of the right to practice for a specified period
* cancellation of registration and removal of the member's name from the register of registered auditors.

The table below provides a summary of the acts or omissions by a registered auditor which will amount to improper conduct.

Rule Reference	***The following will be regarded as improper conduct:***
	Contravention of or failure to comply with:
2.1 2.2 2.5 2.6	* the ***Auditing Profession Act,*** * ***any other Act*** which should be complied with by a Registered Auditor, e.g. Companies Act. * auditing pronouncements prescribed by the IRBA * the IRBA Code of Professional Conduct
	Dishonesty:
2.3	* dishonesty in the form of any offence, especially : - theft, fraud, perjury, bribery and corruption.
2.4	* dishonesty in carrying out work and duties. * dishonesty in relation to any office of trust held by the registered auditor.
2.7	Failure to perform any professional service with ***reasonable care and skill or failure to perform the professional service at all***.
2.8	***Evasion of any tax***, ***duty, levy*** or ***rate*** or assisting others in such evasion by knowingly or recklessly making, signing or preparing false statements or records.
2.9	***Vouching for the accuracy of estimates in future earnings*** The registered auditor's name may not be used in such a manner that it suggests the registered auditor vouches for the accuracy of the forecast. (This lends unwarranted credibility to the forecast.)
	Contraventions in respect of ***trainee accountants***
2.10	* imposing (or attempting to impose) restraints of any kind which will apply after the traineeship However this rule will not apply to restraining a trainee who becomes a registered auditor from soliciting the practitioner's existing clients for a period of one year after the trainee ceases to be employed by the practitioner.
2.11	* requiring compensation for agreeing to the cancellation of a training contract (does not apply to actual expenses paid to IRBA in respect of the training contract).
2.12	* failing in complying with his ***responsibilities to the IRBA/other persons***
2.13	* failing to respond promptly to communications, orders requirements or requests.
2.15	* failing, after demand, to pay fees or other charges due to the IRBA.
	Contraventions in respect of relinquishing engagements
2.14	* failing without reasonable cause to resign from a professional appointment when the client requests the member to do so
2.16	* abandoning his or her practice without giving notice to clients and making necessary arrangements for them to obtain the services they require.
2.17	Acting in a manner which ***brings the profession into disrepute***.

CHAPTER 3

STATUTORY MATTERS

CONTENTS

	Page
INTRODUCTION	3/3
THE COMPANIES ACT NO 71 OF 2008	3/3
1. Introduction	3/3
2. Structure of the Act	3/4
3. Titles of Chapters	3/5
4. Titles of Schedules	3/5
5. Structure of individual sections	3/5
6. Existing companies and compliance with the new Act	3/5
IMPORTANT REGULATIONS FOR STUDY PURPOSES	3/6
SECTION SUMMARIES AND NOTES	3/12
Chapter 1 – Part A – Interpretation	3/12
* Sections covered: 1, 2, 3, 4, 5.	
Chapter 1 – Part B – Purpose and application	3/14
* Sections covered: 7, 8.	
Chapter 2 – Part A – Reservation and registration of company names	3/17
* Section covered: 11.	
Chapter 2 – Part B – Incorporation and legal status of companies	3/18
* Sections covered: 13, 14, 15, 16, 19, 21, 22.	
Chapter 2 – Part C – Transparency, accountability and integrity of companies	3/23
* Sections covered: 23, 24, 26, 27, 28, 29, 30, 32, 33, 34.	
Chapter 2 – Part D – Capitalisation of profit companies	3/27
* Sections covered: 35, 36, 37, 38, 39, 40, 41, 43, 44, 45, 46, 47, 48.	
Chapter 2 – Part E – Securities registration and transfer	3/34
* Sections covered: 49, 50, 51, 52, 53, 55.	
Chapter 2 – Part F – Governance of companies	3/35
* Sections covered: 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 71, 72, 73, 74, 75, 76, 77, 78.	
Chapter 2 – Part G – Winding up of solvent companies and deregistering companies - nil	3/48
Chapter 3 – Part A – Application and general requirement of this chapter	3/49
* Sections covered: 84, 85.	
Chapter 3 – Part B – Company secretary	3/49
* Sections covered: 86, 87, 88, 89.	
Chapter 3 – Part C – Auditors	3/51
* Sections covered: 90, 91, 92, 93.	
Chapter 3 – Part D – Audit committees	3/53
* Section covered: 94.	
Chapter 4 – Public offerings of company securities – nil	3/54
Chapter 5 – Part A – Approval for certain fundamental transactions	3/55
* Sections covered: 112, 113, 114.	
Chapter 5 – Part B – Authority of panel and takeover regulations – nil	3/57
Chapter 5 – Part C – Regulation of affected transactions and offers – nil	3/57
Chapter 6 – Part A – Business rescue proceedings	3/57
* Sections covered: 128, 129, 131.	
Chapter 6 – Part B – Practitioner's functions and terms of appointment	3/59
* Sections covered: 140, 141, 142.	
Chapter 6 – Part C – Rights of affected persons during business rescue proceedings	3/60
* Sections covered: 144, 145, 146, 147, 148.	
Chapter 6 – Part D – Development and approval of business rescue plan	3/61
* Sections covered: 150 to 154.	

Chapter 6 – Part E – Compromise with creditors 3/62
* Section covered: 155.
Chapter 7 – Part A – General principles 3/62
* Sections covered: 156, 158, 159.
Chapter 7 – Part B – Rights to seek specific remedies 3/63
* Sections covered: 161, 162, 163.
Chapter 7 – Parts C to F – nil 3/64
Chapter 8 – Part A – Companies and Intellectual Property Commission 3/64
* Sections covered: 185 to 192 (summary).
Chapter 8 – Part B – Companies Tribunal 3/64
* Sections covered: 193 to 195 (summary).
Chapter 8 – Part C – Takeover regulation panel 3/65
* Sections covered: 196 to 202 (summary).
Chapter 8 – Part D – Financial Reporting Standards Council 3/65
* Sections covered: 203, 204.
Chapter 8 – Part E – Administrative provisions applicable to agencies - nil 3/65
Chapter 9 – Part A – Offences and penalties 3/66
* Sections covered: 213, 214, 215.
Chapter 9 – Part B – Miscellaneous matters – nil 3/66
Chapter 9 – Part C – Regulations etc 3/66
* Section covered: 225

THE CLOSE CORPORATIONS ACT 1984 3/67
1. Introduction 3/67
2. Important changes to the Close Corporations Act 1984 3/67
3. Calculation of the Close Corporations Public Interest Score 3/67
4. Preparation of Financial Statements 3/68
5. Audit requirement 3/68
6. Breakdown of the Close Corporations Act by part 3/68

SECTION SUMMARIES AND NOTES 3/69
Part I - Formation and Juristic Personality 3/69
Part II - Administration of Act 3/69
Part III - Registration, Deregistration and Conversion 3/69
Part IV - Membership 3/71
Part V - Internal Relations 3/73
Part VI - External Relations 3/76
Part VII - Accounting and Disclosure 3/77
Part VIII - Liability of Members and others for the debts of the CC 3/78
Part IX - Winding up - nil 3/79
Part X - Penalties - nil 3/79

THE AUDITING PROFESSION ACT 2005 (ACT 26 OF 2005) 3/80
1. Introduction 3/80
2. Structure of the Act 3/80

SUMMARIES AND NOTES 3/80
Chapter I - Interpretation and objects of the Act 3/80
Chapter II - Independent Regulatory Board for Auditors 3/80
Chapter III - Accreditation and Registration 3/81
Chapter IV - Conduct by and Liability of Registered Auditors 3/83
Chapter V - Accountability of Registered Auditors 3/91
Chapter VI - Offences 3/91
Chapter VII - General Matters 3/92
Appendix - Is it a reportable irregularity? – 10 questions 3/93

INTRODUCTION

Registered Auditors and Chartered Accountants cannot escape the need to have a sound knowledge of the laws and regulations which govern their professional activities as well as the activities of their clients. A knowledge of common law e.g. negotiable instruments, contract etc has to be obtained by all aspirant auditors and accountants during the early years of their study; and in addition hundreds of sections relating to specific disciplines such as income tax and company law must be absorbed. This chapter will concentrate on the more important sections of the Companies Act 2008, the Close Corporations Act 1984 and the Auditing Profession Act 2005. This chapter is ***not*** an in depth study of these Acts – it must rather be regarded as a summary of important sections with brief commentary to be used in conjunction with the Acts themselves.

THE COMPANIES ACT No. 71 of 2008

1. Introduction

1.1 The Companies Act No 71 of 2008 became effective from 1 May 2011. Amendments have been made to it in terms of the Companies Amendment Act No 3 of 2011 and the Financial Markets Act No 19 of 2012. These amendments were not major.

The Companies Regulations 2011 document was also introduced in 2011. The regulations work in tandem with the Companies Act 2008. Section 223 of the Companies Act 2008 gives the Minister of Trade and Industry the power to make these regulations and as a result, they must be complied with in the same manner as the Companies Act itself.

What are the Companies Regulations? The Company Regulations are an extensive set of requirements, explanations and procedures pertaining to the sections of the Companies Act.

Example 1. Sec 30 of the Companies Act states that the financial statements of a public company must be audited ***and*** that any other profit or non-profit company must have its financial statements audited if it is desirable ***in the public interest.***
Regulation 26 supplements and explains this by introducing the concept of a ***public interest score*** and proceeds to lay down how it is calculated.
Regulation 28 then takes the idea further by indicating which companies must be audited based, inter alia, on its public interest score.

Example 2. Sec 21 of the Companies Act states that a person may enter into a written agreement in the name of an entity which is contemplated to be incorporated, but which does not yet exist.
Regulation 35 expands on this and states that a person may give notice to a company of a pre-incorporation contract by filing a notice with the CIPC and delivering to the company a notice in Form CoR35.1. The Regulations also contain an example of Form CoR 35.1.

Example 3. Sec 94(5) of the Companies Act states that the Minister may prescribe minimum qualification requirements for members of an audit committee.
Regulation 42 expands on this and stipulates that "at least one-third of the members of a company's audit committee at any particular time must have academic qualifications, or experience in economics, law, corporate governance, finance, accounting, commerce, industry, public affairs or human resource management. (Very broadly stated and not very onerous!)

Perhaps, fortunately, the Companies Regulations are not important in terms of academic study, as they are more relevant to the application of Company law requirements. However, there are a few important Regulations of which students should have an understanding. These have been dealt with before the section summaries, and where necessary referred to in the notes to the sections.

1.2 In developing the Companies Act 2008, the legislators intention was to produce a Companies Act which would match the changes on the economic, social and political landscape which had taken place since the introduction of the previous Act – The Companies Act No 61 of 1973. Five policy objectives around which the Act would be built were formulated as follows:

Company law should promote the competitiveness and development of the South African economy by:

1.2.1 Encouraging entrepreneurship and enterprise development, and consequently, employment opportunities by
* simplifying the procedures for forming companies; and
* reducing costs associated with the formalities of forming a company and maintaining its existence.

1.2.2 Promoting innovation and investment in South African markets and companies by providing for
* flexibility in the design and organization of companies; and
* a predictable and effective regulatory environment.

1.2.3 Promoting the efficiency of companies and their management.

1.2.4 Encouraging transparency and high standards of corporate governance.

1.2.5 Making company law compatible and harmonious with best practice jurisdictions internationally.

In support of the five objectives, five more specific goals were set as follows:

1.2.6 ***Simplification***

e.g. The Act should provide for a company structure which reflects the characteristics of close corporations such as a simplified procedure for incorporation and more self-regulation.

1.2.7 ***Flexibility***

e.g. Company law should provide for "an appropriate diversity of corporate structures" and the distinction between listed and unlisted companies should be retained.

1.2.8 ***Corporate efficiency***

e.g. Company law should shift from a ***capital maintenance*** regime based on par value, to one based on ***solvency and liquidity***.

e.g. There should be clarification of board structures and director responsibilities, duties and liabilities.

1.2.9 ***Transparency***

e.g. Company law should ensure the proper recognition of director accountability, and appropriate participation of other stakeholders.

e.g. The law should protect shareholder rights, and provide enhanced protections for minority shareholders.

e.g. Minimum accounting standards should be required for annual reports.

1.2.10 ***Predictable Regulation***

e.g. Company law should be enforced through appropriate bodies and mechanisms, either existing or newly introduced.

e.g. Company law should strike a careful balance between adequate disclosure, in the interests of transparency, and over-regulation.

2. Structure of the Act

2.1 Before considering the detail of the sections, it is advisable that you obtain an overall understanding of how the Act is structured:
* the sections are broken down into nine chapters
* each chapter deals with a broadly stated topic

* each chapter is broken down further into alphabetically sequenced parts e.g. Chapter 1 part B.
* each part deals with a more specifically stated topic.
* in addition to the nine chapters, there are five schedules which deal with specific matters.
* the Act itself is then supported by the Companies Regulations 2011.

3. Titles of Chapters

3.1 **Chapter 1.** Interpretation, Purpose and Application (ten sections in Parts A and B).

3.2 **Chapter 2**. Formation, Administration and Dissolution of Companies (seventy three sections in Parts A to G).

3.3 **Chapter 3**. Enhanced Accountability and Transparency (eleven sections in Parts A to D).

3.4 **Chapter 4**. Public Offerings of Company Securities (seventeen sections in a single part).

3.5 **Chapter 5**. Fundamental Transactions, Takeovers and Offers (sixteen sections in Parts A to C).

3.6 **Chapter 6**. Business rescue and Compromise with creditors (twenty eight sections in Parts A to E).

3.7 **Chapter 7**. Remedies and Enforcement (twenty nine sections in Parts A to F).

3.8 **Chapter 8**. Regulatory Agencies and Administration of Act (twenty eight sections in Parts A to E).

3.9 **Chapter 9**. Offences, Miscellaneous Matters and General Provisions (thirteen sections in Parts A to C).

4. Titles of Schedules

1. Schedule 1. Provisions concerning Non-Profit Companies.
2. Schedule 2. Conversion of Close Corporations to Companies.
3. Schedule 3. Amendment of Laws.
4. Schedule 4. Legislation to be enforced by Commission.
5. Schedule 5. Transitional Arrangements.

5. Structure of individual sections

5.1 When reading a section of the Companies Act remember that the majority of the sections deal with:

* the requirements necessary for some action to take place, e.g. appointing an auditor.
* specific prohibition of some action e.g. registering a company name which constitutes the advocacy of hatred based on race, gender or religion, appointing a person who has been prohibited from being appointed a director, as a director.
* the level of authority necessary to make an "action" legal, e.g. a special resolution.
* exceptions/provisos to the requirements of the section or the authority stipulated in the main body of the section.

Thinking about the section in this way makes it easier to understand.

6. Existing companies and compliance with the new Act.

6.1 You may have noticed that Schedule 5 deals with transitional arrangements i.e. transition from the Companies Act 1973 to the Companies Act 2008. In short,

the thousands of companies which existed prior to the introduction of the Companies Act 2008 have continued to operate but are required to comply with the 2008 Companies Act in doing so. A time period has been allowed for companies to align themselves with the requirements of this Act where necessary e.g. replacing the (outdated) Memorandum and Articles of Association with the (new) Memorandum of Incorporation, but in effect the new Act has governed from the date it was proclaimed by the President in the Gazette i.e. 1 May 2011.

IMPORTANT REGULATIONS FOR STUDY PURPOSES

1. Regulations 26, 27, 28, 29 – Public interest scores etc

These regulations work in conjunction with each other and are pertinent to the public interest score concept, audit and review requirements, reportable irregularities for independent reviews as well as the financial reporting standards with which different entities must comply.

Regulation 26.

This regulation introduces the concept of the ***public interest score*** which every company (and close corporation) must calculate at the end of each financial year. The public interest score is used primarily to determine

* which financial reporting standards the company must comply with
* the categories of companies which must be audited/reviewed and
* who must carry out the review of a company which must be independently reviewed.

NOTE (a): The public interest score will be the sum of:

(i) a number of points equal to the average number of employees during the financial year

(ii) 1 (one) point for every R1million (or portion thereof) in third party liability of the company, at the financial year end

(iii) 1 (one) point for every R1million (or portion thereof) in turnover during the financial year

(iv) 1 (one) point for every individual who directly or indirectly has a beneficial interest in any of the company's securities.

Example: The following relevant details pertain to Plus (Pty) Ltd:

	Detail		***Public Interest Points***
1.	Employees at 1 March 01	300	
2.	Employees at 28 Feb 02	360	
3.	Average number of employees	660 ÷ 2	330
4.	Long and short term liabilities at 28 Feb 02 = R8.2m		9
5.	Turnover for the year to 28 Feb 02 R82.7m		83
6.	Shareholders	14	14
	Public Interest Score		436

This illustrative example is straightforward, but the interpretation of the public interest score may be less so. For example:

* if an individual is an employee and a shareholder (direct interest in the company's securities), will he be counted twice in the public interest score?
* if a trust holds shares in a company, is the trust counted as an individual or is it the number of trustees or beneficiaries of the trust or both, which are used in the public interest score?
* similarly, if shares in a company are owned by another company (whether in a holding/subsidiary company or not) does the company holding the shares count as an individual or is it the number of individuals who hold shares in that company, and thereby have a beneficial interest in the shares of the company in which the investment is held? (See note (b) below).
* are temporary or part-time employees included in the public interest score?
* with regard to 3rd party liability, what is a third party?

* if a private company has a subsidiary, is its portion of the subsidiary's turnover included in determining its turnover for public interest score purposes?

No doubt there will be other questions raised pertaining to the interpretation of the "public interest score." Time, practice and case law will eventually resolve these questions.

NOTE (b): In terms of a JSE listing requirement, the subsidiaries of all listed companies must be externally audited regardless of their public interest scores.

Regulation 27

This regulation does two things. ***Firstly,*** it states that a company's financial statements may be compiled ***internally*** or ***independently***.

To be classified as compiled ***independently*** the AFS must be prepared:

* by an independent accounting professional (see Note (a) below)
* on the basis of financial records provided by the company and
* in accordance with any relevant financial reporting standard.

NOTE (a): an "independent accounting professional" means a person who

(i) ***is*** a registered auditor in terms of the Auditing Profession Act ***or***

(ii) ***is a*** member in good standing of a professional body accredited in terms of the Auditing Profession Act i.e. SAICA ***or***

(iii) ***is*** qualified to be appointed as an accounting officer of a close corporation in terms of the Close Corporation Act e.g. a member of SAICA, ICSA,CIMA, ACCA, SAIPA

(iv) ***does not*** have a personal financial interest in the company or a related or inter-related company

(v) ***is not*** involved in the day to day management of the company and has not been so involved during the previous three years

(vi) ***is not*** a prescribed officer, or full-time executive employee of the company (or related or inter-related company) and has not been such an employee or officer during the previous three financial years

(vii) ***is not related*** to any person contemplated in (iv) to (vi) above.

Secondly, regulation 27 stipulates the applicable financial reporting standards with which different categories of company must apply. (Note the requirements for non-profit companies have not been included in this text. Reference can be made to the Regulations themselves if necessary.)

State owned and Profit companies

Category of Companies	***Financial Reporting Standard***
State owned companies.	IFRS, but in the case of any conflict with any requirement in terms of the Public Finance Management Act, the latter prevails.
Public companies listed on an exchange.	IFRS
Public companies not listed on an exchange.	One of – (a) IFRS; or (b) IFRS for SMEs, provided that the company meets the scoping requirements outlined in the IFRS for SME's.

Profit companies, other than state owned or public companies, whose public interest score for the particular financial year is at least 350.	One of – (a) IFRS; or (b) IFRS for SMEs, provided that the company meets the scoping requirements outlined in the IFRS for SME's.
Profit companies, other than state-owned or public companies – (a) whose public interest score for the particular financial year is at least 100 but less than 350; or (b) whose public interest score for the particular year is less than 100, and whose statements are independently compiled.	One of – (a) IFRS; or (b) IFRS for SMEs, provided that the company meets the scoping requirements outlined in the IFRS for SME's
Profit companies, other than state-owned or public companies, whose public interest score for the particular financial year is less than 100, and whose statements are internally compiled.	The Financial Reporting Standard as determined by the company for as long as no Financial Reporting Standard is prescribed.

Regulation 28

This regulation stipulates the categories of companies which are required to be audited. These are:

(i) public companies and state owned companies

(ii) any profit (or non-profit) company which, in the ordinary course of its primary activities, holds assets in a fiduciary capacity for persons who are not related to the company, and the aggregate value of the assets held exceeds R5million at any time during the financial year.

(iii) any company whose ***public interest score*** in that financial year
- * is 350 or more
- * is at least 100 if its annual financial statements for that year were ***internally compiled.***

Note (a): In terms of the JSE listing requirements, all subsidiaries of listed companies must be externally audited regardless of their public interest scores. This is primarily because the holding company's consolidated financial statements must contain audited figures for the audit report to have any value.

Regulation 29

This regulation deals with the matters surrounding the independent review of a company's financial statements (including important regulations pertaining to ***reportable irregularities***).

(i) a company which is ***not required to be audited*** must have an independent review of its annual financial statements unless it is a private company in which every shareholder is a director (owner/managed).

(ii) if the company's public interest score is 100 or more, the review must be conducted by a registered auditor or by a member of a professional body accredited in terms of the Auditing Profession Act (SAICA is currently the only such body).

(iii) if the company's public interest score is less than 100, the review can be carried out by a person who is qualified to be appointed as an accounting officer in terms of the Close Corporations Act, e.g. ACCA, SAIPA, CIMA, SAICA etc.

(iv) the review should be carried out in terms of the International Statement on Review Engagements ISRE 2400.

(v) an independent review of a company's annual financial statements must ***not*** be carried out by an independent accounting professional who was involved in the preparation of the said financial statements (independence requirement).

In terms of Sec 10 of the Close Corporations Act 1984, close corporations must calculate their public interest score (same basis as a company) and may also have to have their financial statements audited.

The following chart summarises which companies and close corporations must be audited, which must be reviewed and which need not bother with external (professional) intervention.

Public interest score	Private company	Close Corporation	Owner Managed
Less than 100	Independent Review regardless of whether AFS are internally or externally compiled. Note (a).	No external intervention (Accounting Officer Report).	No external intervention.
100 to 349	Audit if AFS ***internally*** compiled. Independent Review if AFS externally compiled. Note (b).	Audit if AFS ***internally*** compiled. ***No*** independent review if externally compiled. (Accounting Officer's Report) Note (c).	Audit if AFS ***internally*** compiled. ***No*** independent review if externally compiled. Note (c).
350 and above.	Audit	Audit	Audit

Note (a): This review (less than 100 points) must be carried out by a Registered Auditor or an individual who qualifies for appointment as an Accounting Officer of a close corporation in terms of Sec 60 of the CC Act, e.g. SAICA, SAIPA, ACCA, CIMA etc.

Note (b): ***Audit*** can only be carried out by a Registered Auditor. This ***review*** (100 to 349 points) may only be carried out by a registered auditor or a chartered accountant. Externally compiled means compiled by an "independent accounting professional" as defined.

Note (c): The review for this category of close corporation and owner managed company, is exempt in terms of 30(2A) of the Companies Act 2008.

Note (d): Subsidiary companies of listed companies must be externally audited (JSE listing requirement).

Note (e): All public companies (listed or otherwise) and state owned companies must be audited.

Note (f): Private companies which hold fiduciary assets for persons not related to the company which in aggregate have exceeded R5m at any time during the year, must be audited.

Note (g): A private company may include in its MOI, a clause which requires that it be audited, or a company may be voluntarily audited, e.g. directors decide to have the AFS externally audited.

Regulation 29 - Reportable irregularities, independent reviews.

In terms of the Auditing Profession Act, an auditor is required to report a "reportable irregularity" (as defined) at an ***audit*** client but this requirement does not apply to a ***review*** client. However Regulation 29 places an obligation on the independent reviewer, whether he is a registered auditor or not, to report a reportable irregularity arising at an ***independent review*** client. Whilst the reportable irregularity situations which the auditor or reviewer might find themselves in are very similar, the definitions of a reportable irregularity and the procedure to be followed by the auditor and reviewer, do differ. For the purposes of Regulation 29, the following will apply to reportable irregularities at a review client:

(i) Definition: a reportable irregularity (RI) means any act or omission committed by any person responsible for the management of a company, which
* unlawfully has caused or is likely to cause material financial loss to the company, or to any member, shareholder, creditor or investor of the company in respect of his, her or its dealings with the company or
* is fraudulent or amounts to theft or
* causes or has caused the company to trade under insolvent circumstances.

(ii) Procedure: if an independent reviewer is satisfied or has reason to believe that a reportable irregularity is taking place, he must

* without delay, send a written report to the Commission giving the particulars of the RI and any other information he deems appropriate
* within 3 business days of sending the report to the Commission, notify the Board (of the company) in writing of the sending of the report, and the provisions of this section of Regulation 29.
* a copy of the report must be submitted with this notice to the Board (of the company)
* as soon as reasonably possible but not later than 20 business days from the date the report was sent to the Commission
  - take all reasonable measures to discuss the report with the directors
  - afford the directors the opportunity to make representations in respect of the report
  - send another report to the Commission which must include a statement (with supporting information) that the reviewer is of the opinion that
    - no reportable irregularity has taken place or is taking place ***or***
    - the suspected reportable irregularity is no longer taking place and that adequate steps have been taken for the prevention or recovery of any loss ***or***
    - the reportable irregularity is continuing.

NOTE (a): If the second report states that the reportable irregularity is continuing, the Commission must, as soon as possible after the receipt of the report, notify any appropriate regulator e.g. SARS or SAPS, in writing with a copy of the report.

NOTE (b): For the purposes of investigating or reporting a reportable irregularity, the independent reviewer may carry out whatever procedures he or she deems necessary.

2. Regulation 43 – Social and Ethics committee

2.1 The following companies must appoint a Social and Ethics committee:
* every state owned company
* every listed public company and
* any other company that has in two of the previous five years, scored above 500 points in its public interest score.

2.2 A company which must have a Social and Ethics committee, must appoint the committee within one year of:
* its date of incorporation in the case of a state owned company
* the date it first became a listed public company
* the date it first met the "500 point" requirement.

2.3 The committee must comprise:
* not less than three directors or prescribed officers of the company
* one of which must be a director who is not involved in the day to day management of the company's business (non-executive) and has not been so involved in the previous three years.

2.4 The function of the Social and Ethics committee is to ***monitor*** the company's activities, having regard to any relevant legislation, legal requirements or codes of best practice, with regard to:
* ***social and economic development*** including the company's standing in terms of the goals and purposes of
  - the United Nations Global Compact Principles
  - the OECD recommendations regarding corruption
  - the Employment Equity Act
  - the Broad Based Black Economic Empowerment Act.
* ***good corporate citizenship***
  - promotion of equality, prevention of unfair discrimination and reduction of corruption

- development of communities in which it operates or within which its products are predominantly marketed
- sponsorship, donations and charitable giving.

* ***the environment, health and public safety,*** e.g. the impact of its products/services on the environment**.**

* ***consumer relationships***, e.g. advertising, public relations and compliance with consumer protection laws.

* ***labour and employment***, e.g. compliance with the International Labour Organisation Protocol on decent work and working conditions, and its contribution to educational development.

NOTE (a): A subsidiary company which in terms of the section must appoint a Social and Ethics Committee need not do so, if its holding company has a Social and Ethics Committee which will perform the functions required by Regulation 43 on behalf of the subsidiary.

NOTE (b): The committee must

* draw any matters arising from its monitoring activities to the attention of the board, and

* one of its members must report to the shareholders at the company's AGM.

SECTION SUMMARIES AND NOTES

CHAPTER 1 – Part A – Interpretation

1. SEC 1 – Definitions

NOTE (a): There are numerous definitions. Where necessary these will be dealt with in the section summaries.

2. SEC 2 – Related and inter-related persons and control

For the purposes of the Companies Act 2008:

2.1 An ***individual*** is related to another ***individual*** if
* they are married, or live together in a relationship similar to a marriage or
* they are separated by no more than two degrees of natural or adopted consanguinity (blood relationship) or affinity (relationship between two or more people as a result of somebody's marriage).

2.2 An ***individual*** is related to a ***juristic person*** if :
* the individual directly or indirectly controls the juristic person.

2.3 A ***juristic person*** is related to another ***juristic person*** if :
* either of them directly or indirectly controls the other or the business of the other
* either is a subsidiary of the other or
* a person directly or indirectly controls each of them or the business of each of them.

NOTE (a): The intention of Sec 2 is to prevent individuals or companies from doing things through the medium of another individual or company (entity) which they themselves would not be able to do because of the requirements of the Companies Act. Essentially the Act is saying that an individual or company and the individuals or companies (entities) related to them (as defined by Sec 2) are considered by the Act to be the same person. For example, a company must obtain a special resolution to give a loan to a director. It cannot get around this requirement by giving the loan to the director's wife or child because both the wife and child are related persons as defined in Sec 2. Thus a special resolution will still be required.

NOTE (b): An ***individual*** is defined as a ***natural person***; a ***juristic person*** is a "person" ***formed by law***, e.g. close corporation, trust, and a "person" includes a juristic person.

NOTE (c): The section also provides guidance on what constitutes control:

Example 1. Company B is a subsidiary of Company A. Company A controls Company B. (Sec 2(2)(a)(i))

Example 2. Joe Sope and his wife (related person) control the majority of the voting rights in Company C.
* the control can be by virtue of the two of them owning the majority of the shares ***or*** as a result of a shareholders agreement. (Sec 2(2)(a)(ii))
* Joe Sope and his wife do not have to hold the shares themselves. The shares in Company C could be held by an entity which Joe Sope and his wife control. The control can be ***direct*** or ***indirect***.

Example 3. Fred Bloggs and his son Bob, have the right (by virtue of their combined shareholding) to control the appointment of the directors of Company D who control a majority of the votes at a meeting of the board. (Sec 2(2)(a)(ii)(bb)).

Example 4. Jeeves Ndlovu owns the majority of the members interests (or controls the majority of members votes) in Starwars Close Corporation. (Sec 2(2)(b)).

Example 5. Charlie Weir, the senior trustee of Cape Trust, has in terms of the trust agreement, the ability to control the majority of votes of trustees or appoint the majority of trustees or to appoint or change the majority of the beneficiaries of the trust. (Sec 2(2)(c)).

Example 6. Martin Mars owns the majority interest in both Thunder CC and Lightning CC. The two CCs will be related. (Sec 2(1)(c)(iii)).

NOTE (d): In addition to the specific situations given in the section, there is also a "general" proviso (Sec 2(d)) which suggests that if a person is able to materially influence the policy of a juristic person in a manner comparable to the examples given above, that person will have control.

NOTE (e): Situations/transactions relating to the Act may arise which prejudice a person because ***by definition*** the person is related to the company despite the person having acted totally independently. Sec 2(3) enables the court, the Companies Tribunal (or the Takeover Regulation Panel in the case of a takeover transaction) to exempt the person from the effect of the relationship if there is sufficient evidence to conclude that the person acts ***independently*** of any related person, e.g. although Joan and Peter de Wet are married (and thus by definition are related) they may live apart and may conduct entirely separate business and social lives.

3. SEC 3 – Subsidiary relationships

3.1 A company will be a subsidiary of another juristic person if that juristic person
* is able to directly or indirectly exercise a majority of the voting rights whether pursuant to a shareholders agreement or otherwise or
* has the right to appoint or elect, or control the appointment or election, of directors of that company who control the majority of the votes at a board meeting.

NOTE (a): The holding/subsidiary company relationship is an easy one to understand and it is clear that the companies (holding, subsidiary, sub-subsidiary and fellow subsidiaries) in a group will be "related".

4. SEC 4 – Solvency and liquidity test (important section)

4.1 A company satisfies the solvency and liquidity test if, ***considering all reasonably foreseeable financial circumstances of the company*** at the time
* the assets of the company ***fairly valued*** equal or exceed the liabilities of the company ***fairly valued and***
* it appears that the company will be able to pay its debts as they become due in the ordinary course of business for a period of 12 months after the liquidity and solvency test is considered ***or***
* in the case of a ***distribution*** (see NOTE (e) below), 12 months after the distribution is made.

NOTE (a): This section is very important because it represents a fundamental change to company legislation. The Companies Act 1973 was based upon what was termed the capital maintenance concept which simplistically speaking, resulted in very strict regulations pertaining to any transactions which affected the capital of the company. For example, a company was prohibited from giving financial assistance to anyone for the purchase of shares in that company. A Companies Act based on this concept was regarded as inflexible and over-regulatory. On the other hand the Close Corporations Act has since its inception, been based on the liquidity/solvency test, and has proved to be effective. As has been explained, the legislators and other interested parties required that the new Companies Act be more flexible and accommodating but at the same time sufficiently protective for stakeholders in the company. The Companies Amendment Act 2006 introduced the liquidity/solvency concept for companies and the Companies Act 2008 adopted it. As will become evident, whenever there are important transactions

resulting in outflows of amounts relating in some way to capital/profits, the liquidity/solvency test comes into play. For example, a company can now provide financial assistance to a person to purchase shares in the company provided, inter alia, that the liquidity/solvency requirements are satisfied.

NOTE (b): Where the test is applied, the financial information considered must be based on:
* accurate and complete accounting records as required by the Companies Act Sec 28, and in one of the official languages of the Republic and
* financial statements which satisfy the Companies Act Sec 29 and relevant financial reporting standards.

NOTE (c): The fair valuation of the assets and liabilities must include any reasonably foreseeable contingent assets and liabilities.

NOTE (d): The liquidity/solvency test will also help to protect stakeholders in the company from abuse by the directors (or a majority shareholder) of their powers. The requirements to satisfy the liquidity/solvency test will usually be accompanied by other requirements for the transaction to be legal e.g. permission in the Memorandum of Incorporation and/or a special resolution.

NOTE (e): In terms of a simplified definition, a "distribution" is a direct or indirect transfer by a company of money or other property to a shareholder by virtue of that shareholder's shareholding. For example, a dividend paid to a shareholder is a distribution, but a salary paid to a shareholder who also works in the company is not a distribution. A salary is a payment to an employee. In the context of Sec 4, if a distribution is made, the liquidity/solvency test is only satisfied if the company can pay its debts as they become due in the ordinary course of business for 12 months from when the distribution is made, not from when the decision to make the distribution was taken.

5. SEC 5 – General interpretation of the Act

5.1 Sec 7 (see below) spells out the purposes of the Companies Act 2008. This section states that where interpretation and application of the Act is required, it is to be done in a manner which gives effect to the purposes as stipulated.

5.2 This section also provides an explanation of how a particular number of business days should be calculated, e.g. if a section requires the submission of a document to be within 10 business days of a notification calling for the submission of a document, the 10 business days will be calculated as follows:
* exclude the day of the notification
* include the day by which the document must be submitted
* exclude any public holiday, Saturday or Sunday which falls between the notification date and the date by which the document must be submitted.

5.3 The section also provides guidance on situations where the Companies Act 2008 may conflict with other Acts. (Refer to the Act.)

CHAPTER 1- Part B – Purpose and application

1. *SEC 7 – Purpose of the Act*

1.1 The purposes of this Act are to:
* promote compliance with the Bill of Rights as provided for in the Constitution, in the application of company law;
* promote the development of the South African economy by:
  (i) encouraging entrepreneurship and enterprise efficiency;
  (ii) creating flexibility and simplicity in the formation and maintenance of companies; and

(iii) encouraging transparency and high standards of corporate governance as appropriate, given the significant role of enterprises within the social and economic life of the nation;
* promote innovation and investment in the South African markets;
* reaffirm the concept of the company as a means of achieving economic and social benefits;
* continue to provide for the creation and use of companies, in a manner that enhances the economic welfare of South Africa as a partner within the global economy;
* promote the development of companies within all sectors of the economy, and encourage active participation in economic organization, management and productivity;
* create optimum conditions for the aggregation of capital for productive purposes, and for the investment of that capital in enterprises and the spreading of economic risk;
* provide for the formation, operation and accountability of non-profit companies in a manner designed to promote, support and enhance the capacity of such companies to perform their functions;
* balance the rights and obligations of shareholders and directors within companies;
* encourage the efficient and responsible management of companies;
* provide for the efficient rescue and recovery of financially distressed companies, in a manner that balances the rights and interests of all relevant stakeholders; and
* provide a predictable and effective environment for the efficient regulation of companies.

2. SEC 8 – Categories of companies (important section)

2.1 In terms of this Act two types of companies may be formed and incorporated, namely ***profit*** companies and ***non-profit*** companies.

NOTE (a): A profit company means a company incorporated for the purpose of financial gain for its shareholders.

NOTE (b): A non-profit company means a company that is incorporated for a public benefit, and the property and income of which are not distributable to its incorporators, members, directors, officers or related persons except as reasonable compensation for services rendered.

NOTE (c): A ***profit company*** is either
* a state owned company
* a private company
* a personal liability company or
* a public company.

NOTE (d): a ***private*** company is private because it's Memorandum of Incorporation
* prohibits it from offering any of its securities to the public ***and***
* restricts the transferability of its securities (e.g. an existing shareholder may be required to obtain the consent of the other shareholders if he wishes to sell his shares).

A private company cannot be a state-owned enterprise.

NOTE (e): A ***personal liability*** company
* must meet the criteria for a private company ***and***
* its Memorandum of Incorporation must state that it is a personal liability company. This amounts to a clause in the MOI which provides that the directors and past directors are jointly and severally liable, together with the company, for any debts and liabilities of the company that were contracted during their terms of office.

NOTE (f): A ***public*** company is a profit company which is not a state owned company, a private company or a personal liability company.

NOTE (g): In terms of Sec 11(3)(c) company names must end with the appropriate expression (or abbreviation thereof) which conveys their company category, i.e.

* public company: Anglovaal Limited or Ltd.
* personal liability company: Mitchells' Incorporated or Inc.
* private company: Rubberducks Proprietory Limited or (Pty) Ltd.
* state owned company: Tollroad SOC Ltd.
* non-profit company: Educate NPC

NOTE (h): Although not formally categorized in the Act, a few provisions in the Act recognize two further "types" of company. Both of these "types" of company are exempted from a few requirements of the Act. These "types" are:

* companies where all of the shares are owned by related persons (which results in a diminished need to protect minority shareholders).
* companies where all the shareholders are directors (which results in a diminished need to seek shareholder approval for certain board actions as well as audit requirements in some circumstances).

These are not hugely significant but are in line with the objective of making the Act more flexible.

CHAPTER 2 – FORMATION, ADMINISTRATION AND DISSOLUTION

CHAPTER 2 - Part A –Reservation and registration of company names

1. SEC 11 – Criteria for names of companies

1.1 A company name may
* comprise words in any language, irrespective of whether the words are commonly used or made up together with
  - any letters, numbers or punctuation marks;
  - any of the following symbols +, &, #, @, %, =;
  - round brackets used in pairs to isolate any other part of the name.

1.2 The name of a company must
* ***not*** be the same as or confusingly similar to
  - the name of another company or close corporation
  - a name registered by another person as a defensive name (a name registered to prevent it being used by another person) or a business name in terms of the Business Names Act of 1960, unless the registered user of the defensive name or the business name has officially transferred the name to the company wishing to use it
  - a registered trade mark belonging to a person other than the company
  - a mark, word or expression protected by the Merchandise Marks Act or registered under the Trade Marks Act
* ***not*** falsely imply or suggest, or reasonably mislead a person into believing incorrectly that the company is
  - part of or associated with any other person or entity
  - is an organ of or supported/endorsed by the State, a foreign state, head of state, head of government or international organization.
* ***not*** include any word, expression or symbol, may reasonably be considered to constitute
  - propaganda for war
  - incitement of violence or harm
  - advocacy of hatred based on race, ethnicity, gender or religion.

NOTE (a): Company names must end in the manner which signifies their category. (See Chapter 1 Sec 8. Note (g)).

NOTE (b): In terms of the prohibitions listed in the section, the following company names would probably not be allowed. These are simply illustrative examples.
* Whites Only (Pty) Ltd
* Terrorists for God (Pty) Ltd
* Pick and Pay Enterprises (Pty) Ltd
* Government Supplies (Pty) Ltd
* SARS Consulting Inc
* Zenophobic Solutions (Pty) Ltd
* Bafana Bafana Enterprises (Pty) Ltd

NOTE (c): The Act does allow a profit company to use its company's registration number as its name but, the number must be followed by the expression (South Africa) e.g. 97/3217 (South Africa) (Pty) Ltd. This section appears to have been included so that if a person tries to incorporate a company with a name which is already in use, reserved or contrary to Sec 11(2), the commissioner can use the registration number as the company name ***in the interim***. If the company does not respond, the registration number becomes the name.

NOTE (d): If the company's MOI contains any restrictive condition applicable to the company or prohibits the amendment of any particular provision of the MOI the company's name must be immediately followed by the expression (RF). This alerts any person dealing with the company that the MOI contains restrictions with which the

person should be aware of. Sec 19(5)(a) deems that a person dealing with the company has knowledge of these provisions.

CHAPTER 2 - Part B – Incorporation and legal status of companies

1. SEC 13 – Rights to incorporate company

1.1 One or more persons or an organ of state may incorporate a ***profit*** company.

1.2 Three or more persons or an organ of state or a juristic person may incorporate a ***non-profit*** company.

1.3 The procedure is to
* complete and sign (person or proxy) a Memorandum of Incorporation (MOI)
* file a Notice of Incorporation with a copy of the MOI
* pay the prescribed fee.

NOTE (a): The MOI can be in the prescribed form or can be in a form unique to the company.

NOTE (b): If the MOI includes any provision which imposes a restrictive condition applicable to the company or prohibits the amendment of any particular provision of the MOI, the Notice of Incorporation must include a prominent statement drawing attention to each such provision and its location in the MOI. Remember also that the company's name must be followed by the expression (RF) see Sec 11(3)b.

NOTE (c): The Commission ***may*** reject a Notice of Incorporation if the notice or anything to be filed with it is incomplete or improperly completed ***but*** only if ***substantial compliance*** has ***not*** been achieved.

NOTE (d): Substantial compliance simply means that if a form, document, record etc is in a form or is delivered in a manner that satisfies all the substantive requirements of its required content and delivery, the form or its delivery will be valid (Sec 6).

NOTE (e): The Commission ***must*** reject a Notice of Incorporation if
* the initial directors listed in the notice are fewer than required by the Act;
  - one director for a private company or a personal liability company.
  - three directors for a public company or non-profit company.
* it believes that any of the initial directors as set out in the notice are disqualified in terms of the Act and the remaining directors are fewer than required by the Act.

NOTE (f): Commission is the Companies and Intellectual Property Commission (CIPC).

2. SEC 14 – Registration of company

2.1 As soon as practicable after having accepted a Notice of Incorporation, the Commission must
* assign a unique registration number to the company
* enter the company's information in the Companies Register
* endorse (confirm by official stamp/signature) the NOI and MOI
* issue and deliver to the company, a registration certificate (dated either on date of issue or the date stated in the NOI (if any) by the incorporators, whichever is the later).

NOTE (a): A registration certificate is conclusive evidence that
* all the requirements for incorporation have been complied with and
* the company is incorporated from the date stated on the certificate

3. SEC 15 – Memorandum of Incorporation, shareholder agreements and rules of the company

3.1 Each provision of the MOI
* must be consistent with the Act and
* will be void to the extent that it contravenes or is inconsistent with the Act.

NOTE (a): The MOI deals with numerous matters which are necessary to operate the company. The matters dealt with by the MOI include, inter alia,
* details of the incorporation of the company e.g. date and type of company
* alteration of the MOI
* authorized shares; number and class
* authority of the board to issue debt instruments
* shareholders rights
* shareholders meetings, e.g. notice, location, quorum, resolutions
* directors – composition of the board, meetings, committees, compensation.

NOTE (b): The MOI may include a provision
* dealing with a matter that the Act does not address
* altering the effect of any ***alterable provision*** (see Note (f) below) in the Act e.g. providing for lower quorum requirements for shareholders meetings
* imposing on the company a higher standard, greater restriction, longer period of time or any more onerous requirement than would otherwise apply to the company in terms of an ***unalterable*** provision of this Act. In effect it appears that an unalterable provision can be altered but only if it makes the provision stricter.
* which contains restrictive conditions applicable to the company (including requirements to amend such condition) or which prohibits amendment to any particular provision of the MOI, e.g. the requirement that a special resolution may not be passed by less than 75% of all members votes cannot be altered (the Act allows this percentage to be less).

NOTE (c): In addition to the MOI the board has the authority to make, amend or repeal any necessary or incidental ***rules*** relating to the governance of the company in respect of matters not addressed in the Act or the MOI. These ***rules*** must be:
* consistent with the Act and the MOI otherwise they will be void
* published in terms of the requirements for the publishing of rules contained in the MOI
* filed with the Commission.

NOTE (d): A rule will take effect on a date that is the later of 10 business days after the rule has been filed or the date specified in the rule itself.
* The rule will be binding on an interim basis until the next general shareholders meeting, and on a permanent basis if it is ratified by ordinary resolution.
  If a rule is not ratified, the directors may not make a (substantially) similar rule within 12 months unless it is approved in advance by an ordinary shareholders resolution. Example of a rule: the company may not invest in derivatives.

NOTE (e): A company's MOI and rules are binding
* between the company and each shareholder
* between or among the shareholders of the company
* between the company and
  - each director or prescribed officer or
  - any person serving as a member of any committee of the board.

NOTE (f): An alterable provision is a provision of the Act which can be altered by the MOI of a company. The result of the alteration may be to negate, restrict, limit, qualify, extend or otherwise alter in substance or effect the existing provision of the Act. Some provisions of the Act may ***not*** be altered under any circumstances e.g. a public company cannot decide not to appoint an auditor, but it would appear that a company could, in terms of Sec 15(b) alter this provision by stipulating stricter

audit requirements say, having two different auditors performing the annual audit independent of each other!

NOTE (g): In terms of Sec 15(7), the shareholders of a company may enter into agreements (termed shareholders' agreements) amongst themselves in respect of any matter relating to the company. Any such agreement

* must be consistent with the Act and the MOI
* will be void if it is not consistent

Example: Bob Dobb, Fred Free, and Dave Dimm hold 40, 30 and 30 of the 100 shares in DimDob (Pty) Ltd respectively. The company's MOI states that each share held attracts at least one vote. A shareholders' agreement which states that Bob Dobb's shares attract 80 votes whilst Fred Free and Dave Dimm's shares attract 30 votes each would be acceptable if agreed by all shareholders. In effect this would give control of DimDob (Pty) Ltd to Bob Dobb.

4. SEC 16 – Amending the Memorandum of Incorporation

4.1 A company may amend its MOI.

NOTE (a): The board ***or*** shareholders entitled to exercise at least 10% of the voting rights may propose a ***special*** resolution to make the amendment.

NOTE (b): The company's MOI may provide different requirements with respect to proposals to amend the MOI.

NOTE (c): An amendment to the MOI in compliance with a court order is effected by the board and does not require a special resolution.

NOTE (d): As expected, where an amendment has been made, the company must file a Notice of Amendment with the CIPC with the prescribed fee.

5. SEC 19 – Legal status of companies read in conjunction with *Sec 20 – Validity of company actions.*

5.1 From the date and time that the incorporation of a company is registered, it is a juristic person which exists continuously until its name is removed from the companies register in accordance with the Act. A company has all the legal powers and capacity of an ***individual*** except to the extent that

* a juristic person is incapable of exercising any such power, or having any such capacity e.g. a juristic person cannot exercise the power of an individual to get married!
* the company's Memorandum provides otherwise.

5.2 In terms of Sec 19(1)(c), the company is constituted in terms of the provisions in its MOI. In effect the company is defined by its MOI.

5.3 In terms of Sec 19(2), a person is not ***solely*** by reason of being an incorporator, shareholder or director, liable for any liabilities or obligations of the company, except to the extent that the Act or MOI provides otherwise. In a personal liability company the directors and past directors will be jointly and severally liable, together with the company, for the debts and liabilities of the company contracted during their respective periods of office. (Personal liability companies must contain a clause to this effect in the MOI.)

5.4 In terms of Sec 19(4), a person must not be regarded as having received notice or knowledge of the contents of any document (e.g. MOI, Rules) merely because the document

* has been filed or
* is accessible for inspection at the office of the company

but in terms of Sec 19(5), a person must be regarded as having notice and knowledge of any ***restrictive*** or ***prohibitive*** Sec 15(2)(b) and (c) provisions in the MOI if

* the company's name includes the element RF (refer to notes on Sec 11) and
* the company's Notice of Incorporation or any subsequent Notice of Amendment has drawn attention to the ***restrictive*** or ***prohibitive*** sections.

This is very important for people or companies dealing with a company with (RF) attached to its name – the reason for the (RF) must be followed up.

NOTE (a): In terms of the previous Companies Act 1973, a company was required to state its "main" and "ancillary" objects in its Memorandum. This in a sense defined the capacity of the company and thus any action by the company which appeared to be outside the stated objects of the company, could be challenged as being beyond the capacity of the company and therefore an "ultra vires" act. In terms of the common law ultra vires acts are null and void. For example, could a company which had a main object of being a wholesaler of clothing, take a decision to open a video store, or would that have been an ultra vires act?

The Companies Act 2008 does not require that the company state its "main" and "ancillary" objects, and at the same time gives the company the legal power of an individual. So in terms of the Act there is nothing to prevent a company which sells clothing from opening a video store. Thus the difficulty with "capacity/ultra vires" has been largely removed by the Act (See Note (b)).

NOTE (b): The shareholders of the company can still limit, restrict or qualify the purposes, powers or activities of their company in the Memorandum of Incorporation. For example the MOI may expressly prohibit the company's directors from purchasing financial derivatives (e.g. options or futures). This gives rise to some interesting questions. For example

Q1. If the company purchases futures through XYZ Stockbrokers and subsequently suffers loss, can the company refuse to make good (pay up) on the loss on the grounds that the company had no capacity (it was restricted in the MOI) to purchase the futures and therefore the transaction was null and void?

A1. In terms of Sec 20(1), no action of the company is void by reason only that

* the action was prohibited by the MOI or
* as a consequence of the limitation, the directors had no authority to authorize the action.

Q2. Can the company get out of the transaction on the grounds that XYZ Stockbrokers should have known that the company was prohibited from purchasing futures because the MOI is a public document. (Constructive Notice)?

A2. In terms of Sec 19(4), a person is not deemed to have knowledge of the contents of a document merely because the document

* has been filed or
* is accessible for inspection.

Furthermore in terms of Sec 20(7), XYZ Stockbrokers are entitled to presume that the company complied with all of the formal and procedural requirements (such as obtaining authority) in terms of the Act, the company's MOI and rules unless

* they know or reasonably ought to have known, that the company had failed to comply with the requirement.

However both the answers to Q1 and Q2 are influenced by Sec 19(5) which states that a person (XYZ Stockbrokers) must be regarded as having knowledge of restrictive provisions in the company's MOI if the company's name contains the element (RF) which it should!

Q3. Can the shareholders ratify (approve) an action by the company or the directors which is actually restricted by the MOI? For example, could the shareholders ratify the directors action of purchasing the futures?

A3. Yes. In terms of Sec 20(2), they may ratify the action by special resolution. (Note: an action which is in contravention of the Companies Act cannot be ratified).

Q4. Can a director who discovers that his fellow directors (the company) are about to carry out an action which is prohibited by the MOI, restrain (prevent) the company from doing so? e.g. prevent the directors from purchasing futures from XYZ Stockbrokers?

A4. Yes. In terms of Sec 20(5), one or more shareholders or directors may take proceedings to restrain the company.

Q5. Do the shareholders have a claim for damages against a director who causes the company to do anything inconsistent with the Act or any restrictions etc in the MOI or rules? e.g. can a shareholder sue the directors for losses suffered in the futures transaction with XYZ Stockbrokers?

A5. Yes. Sec 20(6). This section says that each shareholder of a company has a claim for damages against any person who intentionally, fraudulently or due to gross negligence, causes the company to do anything which is inconsistent with the Act or with a limitation, restriction, or qualification in the MOI or rules, unless the action has been ratified by the shareholders.

6. SEC 21 – Pre-incorporation contracts

6.1 A person may enter into a written agreement in the name of, or purport to act in the name of, or on behalf of an entity which has not yet been incorporated (does not exist).

NOTE (a): This section is necessary, because prior to incorporation the company does not exist as a juristic person and therefore cannot exercise its powers.

NOTE (b): Within three months after its date of incorporation, the board of the company may
* completely, partially or conditionally ratify or reject the pre-incorporation contract.

NOTE (c): If the company fails (takes no action) to ratify or reject the pre-incorporation contract, the company will be ***deemed*** to have ratified the contract.

NOTE (d): Although the other party should always be cautious when entering a pre-incorporation contract, the section does provide some protection;
* firstly, the person who purported to be acting on behalf of the company yet to be incorporated, is jointly and severally liable with any other such person for all liabilities created while so acting if
  - the entity is ***not*** incorporated or
  - the entity once incorporated, rejects the contract (or any part thereof).

7. SEC 22 – Reckless trading prohibited

7.1 A company must not
* carry on its business recklessly, with gross negligence, with intent to defraud any person or for any fraudulent purpose.

NOTE (a): If the Commission (Companies and Intellectual Property Commission) has reasonable grounds to believe that a company is contravening this section or is unable to pay its debts as they become due and payable in the normal course of business, the Commission may issue a notice to the company to show cause why the company should be permitted to continue carrying on its business or trade.

NOTE (b): The company has 20 business days in which to satisfy the Commission that it is not contravening the section or that it can pay its debts. If the company does not achieve this, the Commission may issue a compliance notice requiring it to cease trading.

NOTE (c): This section may prove cumbersome to implement but has been included so that the Commission has the power to intervene against errant companies.

CHAPTER 2 - Part C - Transparency, accountability and integrity of companies

1. SEC 23 – Registered office

1.1 Sec 23(3). Every company must continuously maintain at least one office in the Republic.

NOTE (a): The company must register the address of its office when filing its Notice of Incorporation. If the address changes, the company must file a notice of change with the prescribed fee.

NOTE (b): This section deals extensively with external companies.

2. SEC 24 – Form and standards for company records

2.1 A company must keep all documents, accounts, books, writing, or other information which it is required to keep in terms of this Act or any other public regulation
* in written form or
* in electronic or other form which allows it to be converted to written form within a reasonable time and they must be kept
* ***for a period of*** seven years (or any longer period if so specified by other applicable regulations).

2.2 Every company must maintain
* a copy of its Memorandum of Incorporation (including amendments) and any Rules the company has made
* a record of its directors (see note (c) below)
* copies of all reports presented at an annual general meeting
* copies of annual financial statements
* accounting records as required by the Act
* notice and minutes of shareholders meetings, including all resolutions adopted and supporting documentation made available to the holders of securities related thereto
* copies of any written communications sent to shareholders (all classes of shares)
* minutes of all meetings of directors, or directors' committees and of the audit committee.

NOTE (a): every ***profit*** company must maintain a securities register (see note to Sec 50).

NOTE (b): every ***profit*** company must maintain a register of its company secretary and auditors if they have made such appointments (not all profit companies are obliged to have a company secretary or auditor).

NOTE (c): The company's record of directors must include for each director
* full name and any former names
* identity number or if no ID number, date of birth
* if not a South African, nationality and passport number
* occupation
* date of most recent appointment as a director
* name and registration number of every other company (including a foreign company) of which the person is a director, and in the case of a foreign company, its nationality.

NOTE (d): In terms of Sec 25, the company's records should be accessible at the company's registered office or from other locations in the Republic
* if the records are not at the registered office, or are moved from one location to another, the company must file a notice of location of records.

NOTE (e): In terms of Regulation 23, a company's record of directors must include, with respect to each director
* the address for service for that director
* in the case of a company that is required to have an ***audit committee*** e.g. public company, any professional qualifications and experience of that director to enable the company to comply with the qualification requirements for an audit committee,

3. SEC 26 – Access to company records

3.1 A person who holds or has a beneficial interest in any securities issued by a company has a right to ***inspect*** and ***copy*** information contained in the records of the company as listed in Sec 24 para 2.2 above (but see Note (a) below).

3.2 Such a person also has a right to any other information to the extent granted by the Memorandum of Incorporation.

NOTE (a): This right of access does ***not*** extend to the minutes of meetings and resolutions of directors, directors' committees or the audit committee ***or*** to the ***accounting records***.

NOTE (b): The right of access in terms of this section is in addition to any right arising from Sec 32 of the Constitution, the Promotion of Access to Information Act or any other public regulation.

NOTE (c): It will be an offence by the company if it fails to accommodate any reasonable request for access or to refuse, impede, interfere with or attempt to frustrate any person entitled to information, from exercising his rights.

NOTE (d): In terms of Sec 31, a person who holds securities in a company is entitled to receive a notice of publication of the AFS, and on following the required steps to receive, without charge, one copy of the AFS.

4. SEC 27 – Financial year of company

4.1 The company must have a financial year
* the year-end date must be stated in the Notice of Incorporation
* the financial year will be the company's accounting period
* a company may change its year-end by filing a notice of that change, but not to a date prior to the date on which the notice is filed.

5. SEC 28 – Accounting records

5.1 A company must keep accurate and complete accounting records in one of the official languages of the Republic.

NOTE (a): Records must satisfy the requirements of the Act and any other law to facilitate the preparation of financial statements, and must include any prescribed accounting records e.g. fixed asset register.

NOTE (b): Accounting records must be kept at or be accessible from the company's registered office.

NOTE (c): If a company, with ***an intention to deceive or mislead any person***
* fails to keep accurate or complete records or

* keeps records other than in the prescribed manner and form or
* falsifies or allows its records to be falsified

it will be guilty of an offence.

6. SEC 29 – Financial statements

6.1 If a company provides any financial statements (including AFS) to any person, for any reason, those statements must:

* satisfy the ***financial reporting standards*** as to form and content
* ***present fairly*** the state of affairs and business of the company, and explain the transactions and financial position of the business
* show the company's ***assets, liabilities and equity*** as well as its ***income and expenses***
* set out the ***date of publication*** and the ***accounting period*** of the statements
* prominently indicate on the first page of the statements whether the statements
  - have been audited or
  - independently reviewed or
  - have ***not*** been audited or independently reviewed
  - the name and professional designation if any, of the individual who prepared or supervised the preparation of, those statements.

NOTE (a): Financial statements must not be false, misleading or incomplete in any material respect.

NOTE (b): Any person (e.g. financial director), who is party to the preparation, approval, dissemination or publication of financial statements which do not comply with (6.1) above or which are materially false or misleading, will be guilty of an offence.

NOTE (c): This section gives the Minister power to prescribe financial reporting standards. These standards must be consistent with the International Financial Reporting Standards (IFRS). See Companies Regulations 27.

NOTE (d): A ***summary*** of the financial statements may be provided by the company, but the first page of the summary must prominently state

* that the document is a summary, and identify the financial statements which have been summarized
* whether the financial statements which have been summarized were audited, independently reviewed or neither
* the name and professional designation (if any) of the individual who prepared or supervised the preparation of the financial statements which have been summarized
* the steps required to obtain a copy of the financial statements which have been summarized.

NOTE (e): Sec 29 gives legal force to the accounting standards, e.g. IFRS, IFRS for SMEs.

7. SEC 30 – Annual financial statements

To understand the requirements of Sec 30 of the Companies Act 2008 it is necessary to understand ***Regulations 26 to 29***. The important points pertaining to ***Section 30*** are included in the summary below. The discussion on the pertinent regulations is at the start of the chapter. We recommend that you work through the section and the Regulations concurrently.

7.1 A company must prepare annual financial statements within ***six*** months after the end of the financial year.

7.2 In the case of a ***public*** company, the financial statements must be ***audited.***

7.3 In the case of ***any other profit (or non-profit) company*** the financial statements ***must*** be

* audited if so required by Regulation 28

* audited voluntarily if the MOI, or a shareholders resolution or the Board requires it or
* independently reviewed in terms of Regulation 29.

NOTE (a): In terms of his powers granted in Sec 30(7) of the Companies Act, the Minister has, in Regulation 28 and 29 prescribed which categories of companies must be audited and which companies must be independently reviewed. This categorization is based upon the public interest score of the company as explained in Regulation 26.

NOTE (b): A voluntary audit may arise from a requirement in the company's MOI, an ordinary shareholders resolution or a decision by the board.

NOTE (c): The requirements of the "independent review" have been formulated by the Minister in Regulation 29.

NOTE (d): A company will be exempted from the requirement to be ***audited*** or ***independently reviewed*** if

* every person who is a shareholder (security holder) is also a director of the company

unless the company falls into a class of company that is required to have its annual financial statements audited in terms of the Regulations, e.g. it has a public interest score of more than 350.

NOTE (e): The annual financial statements must

* include an auditor's report (if audited)
* a directors report dealing with the state of affairs, the business and profit and loss of the company, any matter material for the shareholders to appreciate the company's state of affairs and any prescribed information
* be approved by the board and signed by an authorized director (usually managing director/chief executive officer)
* be presented at the first shareholders meeting after the financial statements have been approved by the board.

NOTE (f): The annual financial statements of a company which is required to have its statements audited, must include

* the amount of remuneration and benefits received by each director
* pensions paid and payable to past and present directors or to a pension scheme for their benefit
* amounts paid in respect of compensation paid for loss of office
* the number and class of any securities issued to a director or a person related to the director (related as defined) and the consideration received by the company
* details of service contracts of current directors.

NOTE (g): The term remuneration is all embracing and includes

* fees, salary, bonuses, performance related payments
* expense allowances (for which the director is not required to account)
* contributions paid under any pension scheme not otherwise disclosed
* value of options given directly or indirectly to a director, past or future director or person related to them
* financial assistance for the purchase of shares to any director, past or future director or person related to them
* with respect to any financial assistance or loan made the amount of any interest deferred, waived or forgiven or the difference between the amount of interest that would reasonably be charged in comparable circumstances at fair market rates in an arms length transaction and the interest actually charged, if the actual interest is less, e.g. fair market rate on R1m loan is 10%, loan granted to director at 2%, therefore disclose R80 000 remuneration.

NOTE (h): This disclosure is also applicable to prescribed officers of the company.

NOTE (i): A person who holds or has a beneficial interest in any security of a company is entitled to receive:
* without a notice of the publication of the AFS setting out the steps required to obtain a copy
* on demand, without charge one copy of the AFS.

8. SEC 32 – Use of company name and registration

8.1 A company must provide its full registered name or registration number to any person on demand, and not misstate its name or registration number in a manner likely to mislead or deceive any person.

8.2 A person must not use the name or registration number of a company in a manner likely to convey the impression that the person is acting on behalf of the company unless authorized to do so by the company.

8.3 Every company must have its name or registration number mentioned in legible characters in all notices and official publications of the company and in all bills of exchange, promissory notes, cheques, orders for money or goods and in all letters, delivery notes, invoices, receipts and letters of credit.

9. SEC 33 – Annual return

9.1 Every company must file an annual return in the prescribed form with the prescribed fee and within the prescribed period after its financial year-end.

10. SEC 34 – Additional accountability requirements for certain companies

10.1 Public companies and state owned companies must comply with Chapter 3 of the Companies Act 2008.

10.2 Private companies, personal liability companies and non-profit companies are not required to comply except to the extent the MOI provides otherwise (i.e. voluntary adoption).

NOTE (a): Chapter 3 makes it obligatory for a public company to appoint
* an auditor
* an audit committee
* a company secretary.

CHAPTER 2 - Part D – Capitalisation of profit companies

1. SEC 35 –Legal nature of company shares and requirement to have shareholders

1.1 A share is movable property, transferable in any manner provided for in the Act (or other legislation).

1.2 A share does ***not*** have a nominal or par value.

1.3 A company may not issue shares to itself.

1.4 An ***authorized*** share has no rights associated with it ***until*** it has been issued.

NOTE (a): The concept of a ***par value*** share has been abandoned. There are thousands of companies which currently have par value shares in issue; these shares retain the description and rights they had prior to the introduction of the new Act but will in

due course have to be "converted" to no par value shares in terms of the transitional arrangements.

2. SEC 36 – Authorization for shares

2.1 The company's Memorandum of Incorporation ***must*** set out
* the classes and number of shares that the company is authorized to issue
* a distinguishing designation (name) for each class of share
* the preferences (e.g. to dividends), rights (e.g. voting) and limitations (e.g. aspects of voting), applicable to each class of share.

NOTE (a): The Memorandum ***may*** authorize a stated number of unclassified shares for subsequent classification by the board, and may set out a class of shares without specifying its preferences, rights and limitations. Obviously before issue, all of the above must be determined (by the board).

NOTE (b): The authorization, classification and number of authorized shares as well as the preferences, rights and limitations may be changed only by
* an amendment to the Memorandum of Incorporation by ***special resolution or***
* the board of the company (but see NOTE (c)).

NOTE (c): Except to the extent that the MOI provides otherwise, the board may
* increase or decrease the number of authorized shares for any class of shares
* reclassify any classified authorized but unissued shares
* classify any unclassified shares (NOTE (a)) and
* determine the preferences, rights and limitations of any shares described in NOTE (b)

If any of the above actions are carried out by the directors, the MOI must still be amended (i.e. file a notice of amendment).

3. SEC 37 – Preferences, rights, limitations and other share terms

3.1 All the shares within a class of shares will have the same preferences, rights and limitations as other shares in that class.

3.2 Each issued share of a company has a general voting right (a general voting right is a vote which can be exercised "generally at a shareholders' meeting"), unless the MOI provides otherwise. This is interpreted to mean that a voting right can be limited but not taken away entirely. (See note (a)).

NOTE (a): On a matter which affects the preferences, rights or limitations of a share, the shareholder of that share has an irrevocable right to vote on that matter. (The MOI cannot change this.)

NOTE (b): If the company has only ***one class of share***
* the shareholder has a right to vote on every matter to be decided by the shareholders and is
* entitled to receive the net assets of the company upon its liquidation.

NOTE (c): If the company has ***more than one class of share***, the MOI must ensure
* at least one class of share has voting rights for each particular matter which may be submitted to the shareholders; (note that all classes may be entitled to vote on all matters but not necessarily)
* at least one class of share is entitled to receive the net assets of the company on its liquidation (note again that all classes may be entitled to a portion of the net assets).

NOTE (d): The company's MOI may
* confer special, conditional or limited voting rights

* provide for redeemable or convertible shares, specifying for example, how the share will be redeemed, when it will be redeemed, how the price will be determined, etc.
* entitle the shareholders to distributions (e.g. dividends) calculated in any manner, and designed as cumulative, non-cumulative etc
* designate a share as preferent (over other classes) with regard to dividends and other distributions.

NOTE (e): If the preferences, rights or limitations attached to a share have been materially and adversely altered, a holder may apply for relief (Sec 164 covered later).

4. SEC 38 – Issuing shares

4.1 The board of the company may issue shares at any time (shares must be ***authorized*** etc in the MOI).

NOTE (a): If the board issues shares which have not been authorized or which are in excess of the number of authorized shares per the MOI, the issue can be retroactively authorized within 60 business days (this will be by special resolution).

NOTE (b): If this resolution is not passed, the issue is null and void to the extent that authorization has been exceeded. Subscribers must be repaid including interest, and all share certificates (and entries in the share register) must be nullified.

NOTE (c): A director who was party to the issue may be liable for any loss suffered by the company as a result of the invalid issue.

5. SEC 39 – Subscription of shares

5.1 If a ***private*** company proposes to issue shares, each (existing) shareholder, has a right, before any person who is not a shareholder, to be offered, and within a reasonable time, to subscribe for a percentage of the shares to be issued, equal to the voting power of that shareholder's general voting rights, immediately before the offer was made, e.g. Joe Egg has general voting rights to 35% of the company's shares. The company wishes to issue 1000 shares. Joe Egg has a pre-emptive right to 350 shares but could also decide to subscribe to a lesser number of shares e.g. 150 shares.

5.2 A company's MOI may limit, negate, restrict or place conditions upon this pre-emptive right.

6. SEC 40 – Consideration for shares

6.1 The board may issue authorized shares only
* for ***adequate*** consideration as determined by the board or
* in terms of existing conversion rights or
* as a capitalization issue.

NOTE (a): The consideration determined by the directors cannot be challenged on any basis other than the directors did ***not*** act in good faith, in the best interests of the company and with the degree of skill and diligence reasonably expected of a director.

NOTE (b): Only once a company has received the consideration, will the share be considered to be fully paid. Once issued and paid, the shareholders details must be entered in the "securities register".

7. SEC 41 – Shareholders approval for issuing shares in certain cases

7.1 If a share (option, security convertible into a share etc) is to be issued to
* a director, future director, prescribed officer, or future prescribed officer

* a person related or inter-related to the company or to a director, future director etc or
* a nominee of any of these persons, the issue must be approved by ***special resolution*** of the shareholders.

NOTE (a): Don Ndungane is a director of Wingerz (Pty) Ltd. The board wishes to issue shares to:

i. Don Ndungane – special resolution
ii. Mary Ndungane (Don's wife) – special resolution
iii. Dons (Pty) Ltd – (company controlled by Don and his wife) – special resolution
iv. Mike Zuma as nominee to Don Ndungane (Mike Zuma is Don Ndungane's second cousin) – special resolution because of nominee relationship (not because of family connection).

NOTE (b): The special resolution requirement will ***not*** be required where the issue

* is under an agreement underwriting the shares (etc).
* in proportion to existing holdings on the same terms and conditions as have been offered to all shareholders (or to all shareholders of the class of shares being issued).
* is the fulfilment of a pre-emptive right
* is pursuant to an employee share scheme
* is an offer to the public.

NOTE (c): A "future" director or prescribed officer who becomes a director or prescribed officer more than six months after the issue, is not considered a "future" director or prescribed officer, for the purposes of this section.

8. SEC 43 – Securities other than shares

8.1 The board may authorize the issue of debt instruments except to the extent provided by the MOI (e.g. convertible debenture).

8.2 Debt instrument can be unsecured or secured.

8.3 Other than to the extent provided by the MOI, a debt instrument may grant special privileges to the holder e.g.

* attending and voting at general meetings
* voting on the appointment of directors
* redemption of the instrument or conversion to shares.

9. SEC 44 – Financial assistance for subscription of securities

9.1 A company may provide financial assistance to any person for the purchase of any security (share etc) of the company itself or a related company e.g. holding company, ***provided***

* any conditions or restrictions in respect of the granting of financial assistance set out in the Memorandum of Incorporation are adhered to and
* the board is satisfied that
  - immediately after providing the financial assistance, the company would satisfy the liquidity/solvency test
  - the terms under which the financial assistance is proposed, are fair and reasonable to the company
* a ***special resolution*** is obtained (See Note (d)).

NOTE (a): The requirements of this section do not apply to a company whose primary business is the lending of money.

NOTE (b): Financial assistance can be a loan, guarantee, provision of security.

NOTE (c): If financial assistance is given in contravention of this section or the MOI, the transaction will be void and a director will be liable for any losses incurred by the company, if

* the director was present at the meeting when the board approved the resolution, or participated in the making of the decision and
* failed to vote against the resolution knowing that the provision of financial assistance was inconsistent with the Act or MOI.

NOTE (d): The special resolution must have been passed within the previous 2 years. The approval given by the special resolution can be for a specific recipient, or generally for a category of potential recipients.

NOTE (e): If the financial assistance is pursuant to an employee share scheme, a special resolution is ***not*** required (other requirements must be satisfied).

NOTE (f): The MOI (or company or board) cannot permit the granting of financial assistance in contravention to this section e.g. the MOI cannot contain a clause and the directors cannot pass a resolution which overrides the requirement to apply the liquidity/solvency test.

10. SEC 45 – Loans or other financial assistance to directors

10.1 A company may provide, direct or indirect financial assistance (for any purpose) to

* a director of the company or a related company e.g. holding company, or
* to a related or inter-related company, or corporation or
* to a member of a related or inter-related corporation or
* to any such person related to such corporation, company, director, prescribed officer or member ***provided***
* any conditions or restrictions in respect of the granting of financial assistance set out in the MOI are adhered to and
* the board is satisfied that
  - immediately after providing the financial assistance, the company would satisfy the liquidity/solvency test
  - the terms under which the financial assistance is proposed, are fair and reasonable to the company
* a ***special resolution*** is obtained (see Note (d) below).

NOTE (a): The requirements of this section do not apply to

* a company whose primary business is the lending of money
* financial assistance in the form of an accountable advance to meet
  - legal expenses in relation to a matter concerning the company or
  - anticipated expenses to be incurred by the person on behalf of the company or
  - amounts to defray the recipient's expenses for removal (relocation) at the company's request.

NOTE (b): Financial assistance can be a loan, guarantee, provision of security.

NOTE (c): If financial assistance is given in contravention of this section or the MOI, the transaction will be void and a director will be liable for losses suffered by the company, if

* the director was present at the meeting when the board approved the resolution or participated in making such decision and
* failed to vote against the resolution, despite knowing that the provision of financial assistance was inconsistent with the Act or the MOI.

NOTE (d): The special resolution must have been passed within the previous two years. The approval given by the special resolution can be for a specific recipient or generally for a category of potential recipients.

NOTE (e): If the loan is made to a director pursuant to an employee share scheme, a special resolution is not required (other requirements must be satisfied).

NOTE (f): The MOI (or company or board) cannot permit the granting of a loan in contravention to this section, e.g. the MOI cannot contain a clause, and the directors cannot pass a resolution which overrides the requirement to apply the liquidity/solvency test.

NOTE (g): Where the board adopts a resolution to provide financial assistance (as contemplated by this section), the company must provide written notice of the resolution to all shareholders (unless every shareholder is a director) ***and to*** any trade union representing the company's employees.

* If the total value of all financial assistance given within the financial year exceeds one-tenth of 1% of the company's net worth at the time of the resolution, this notice must be given within ***10 business days*** of the adoption of the resolution
* if the total value does not exceed one tenth of 1% of net worth, the notice must be given within 30 days after the end of the financial year.

NOTE (h): This section is much simpler than its predecessor (Companies Act 1973 Sec 226) but is still cast very wide. The intention is to control abuse by the directors by, for example, making loans to themselves which are not in the interests of the company. The section does not seek to prejudice the directors but rather to control them. The section seeks to control financial assistance to a director in whatever "form" that director may be e.g. a close corporation or company controlled by the director, a person related (as defined) to the director such as his wife. The section also covers directors of companies related to the company granting the loan e.g. its holding company, subsidiary or fellow subsidiary.

NOTE (i): The section also applies to "prescribed officers" of the company.

11. SEC 46 – Distributions must be authorized by the board

11.1 A "distribution" has a defined meaning in the context of the Act. It amounts to a transfer of money or other property to or for the benefit of one or more holders on any of the shares of the company or of another company within the same group of companies. A person receives a "distribution" by virtue of being a shareholder.

11.2 Examples are

* dividends
* payments in lieu of capitalization shares
* share "buy backs"
* incurring a debt for the benefit of a shareholder
* cancelling a debt owed by a shareholder (forgiveness).

11.3 A company must not make a distribution unless the distribution

* is pursuant to an existing legal obligation or court order ***or***
* the board of the company has passed a resolution authorizing the distribution ***and***
* it reasonably appears that after the distribution, the company will satisfy the liquidity and solvency test ***and***
* the board resolution states that the directors applied the liquidity and solvency test and reasonably concluded that the requirements of the test were satisfied.

NOTE (a): If a distribution has not been carried out within 120 business days of making the resolution, the board must ***reconsider*** the liquidity and solvency of the company and may not proceed with the distribution unless a further resolution is taken to make the distribution. The resolution must again acknowledge that the directors carried out the liquidity and solvency test.

NOTE (b): If a director was present at the meeting, or participated in the making of the decision to make the distribution and failed to vote against it knowing that it was contrary to the requirements of this section (Sec 46), he may be liable for any loss, damage or cost sustained by the company.

12. SEC 47 – Capitalization shares

12.1 Except as the MOI provides otherwise the board may, by resolution, approve the issuing of any authorized shares of the company as capitalization shares on a pro-rata basis to existing shareholders.

NOTE (a): When resolving to award a capitalization share, the board may permit a shareholder to receive a cash payment instead at a value determined by the board. This would amount to a distribution and require the application of the liquidity and solvency test by the directors.

13. SEC 48 – Company or subsidiary acquiring company's shares

13.1 A company may acquire (buy back) its own shares. This will be a distribution as defined and the requirements of Sec 46 must be satisfied (board resolution, liquidity/solvency requirements).

13.2 A subsidiary of a company may acquire shares of its holding company but
* not more than 10% of the total issued shares of any class may be held by all of the subsidiaries of that holding company taken together and
* the voting rights attached to the shares held by the subsidiary(ies) ***may not be exercised*** while held by the subsidiary (whilst it remains a subsidiary).

NOTE (a): Where a buy back has taken place, the stated capital must be reduced by the amount arrived at by using the following "formula":

$$\text{Number of shares acquired} \times \frac{\text{stated capital}}{\text{number of issued shares}}$$

If there are various classes of shares, the formula will be applied by class of share.

NOTE (b): The share certificates pertaining to the shares acquired will be cancelled and will revert to the status of authorized shares.

NOTE (c): If the company acquires any shares contrary to Sec 46 or this section (Sec 48) the company must, not more than two years after the acquisition, apply for a court order to reverse the acquisition. The court may order that
* the person from whom the shares were acquired return the amount paid by the company and
* the company re-issues an equivalent number of shares of the same class.

NOTE (d): A director of the company will be liable for any loss, damages or costs arising from an acquisition of shares contrary to Sec 46 or Sec 48 if
* he was present at the meeting when the board approved the acquisition or he participated in the making of the decision and
* failed to vote against the acquisition despite knowing it was contrary to Sec 46 or Sec 48.

NOTE (e): A decision by the board to "buy back" shares held by a ***director*** or prescribed officer or a person related to the director or prescribed officer must be approved by a ***special resolution***.

If any buy back involves the acquisition of more than 5% of the issued shares of any particular class of the company's shares, the decision is subject to the requirements of Sec 114 and 115 which deal with "schemes or arrangements."

CHAPTER 2 – Part E - Securities registration and transfer

1. SEC 49 – Securities to be evidenced by certificates or uncertificated

1.1 Any security (e.g. share) must either be
* certificated (evidenced by the issue of a certificate)
* uncertificated (no certificate issued).

NOTE (a): Simplistically stated, a hard copy certificate will be issued by the company when a security is ***certificated***. Where the security is ***uncertificated*** its details will be held in a central securities depository database.

NOTE (b): Whether a security is ***certificated*** or ***uncertificated*** does not affect the rights and obligations attaching to the security.

2. SEC 50 –Securities register and numbering

2.1 Every company must establish and maintain a register of its issued securities which contains the details of the security and the holder, and any "transfers" of securities.

NOTE (a): Where a company issues uncertificated securities, a record is maintained (usually) by a central securities depository and this acts as the company's uncertificated securities register.

NOTE (b): Unless all the shares of a company rank equally for all purposes, the shares or each class of shares must be distinguished by an "appropriate numbering system".

3. SEC 51, 52 and 53 – Registration and transfer of certificated and uncertificated securities

3.1 A certificate evidencing any certificated security must state on its face
* name of the issuing company
* name of the person to whom security was issued
* number and class and designation, if any, of the share being issued
* any restrictions on transfer.

NOTE (a): The certificate must be signed (manually or by electronic or mechanical means) by two persons authorized by the company's board.

NOTE (b): In the absence of evidence to the contrary, the certificate is satisfactory proof of ownership.

3.2 A company which has its uncertificated securities administered by a central securities depository, may request the depository to furnish it with all details of that company's uncertificated securities reflected on the depository's database.

NOTE (c): A person who holds a beneficial interest in any security of the company and who wishes to inspect the uncertificated securities register, may do so but must do it
* through the relevant company and
* in accordance with the rules of the central securities depository.

The depository must, within five business days, produce a record of the company's uncertificated securities register reflecting the name and address of the persons to whom securities were issued, the number of securities issued to them, and any other recorded details pertaining to the security e.g. restrictions on transfer.

NOTE (d): The transfer of uncertificated securities held in an uncertificated securities register may only be effected by the depository
* on receipt of an authenticated instruction ***or***
* an order of court.

The transfer must comply with the rules of the depository.

4. SEC 55 – Liability relating to uncertificated securities

4.1 A person who takes any unlawful action which results in any of the following, with regard to the securities register or uncertificated securities ledger, is liable to any person who has suffered any direct loss or damage arising from that unlawful action;

* the name of any person (unlawfully) remains in the register or is removed or omitted.
* the number of securities is (unlawfully) increased, reduced or left unaltered.
* the description of the securities is (unlawfully) changed.

CHAPTER 2 - Part F - Governance of companies

1. SEC 57 – Interpretation and application of this part

1.1 In this part a shareholder is defined as any person who is entitled to exercise any voting right irrespective of the form, title or nature of the security to which the voting right attaches.

1.2 This section recognizes certain ownership/directorship arrangements which exist in some companies, and seeks to simplify the governance of those companies.

* If a ***profit*** company has only ***one shareholder***, that shareholder may exercise any or all of the voting rights pertaining to any matter, at any time without notice or compliance with internal formalities, except to the extent that the MOI provides otherwise.
* If a ***profit*** company has only ***one director***, that director may exercise or perform any function of the board at any time without notice or compliance with internal formalities except to the extent the MOI provides otherwise.
* If ***every shareholder*** of a company is also a ***director*** of that company, any matter that is required to be referred by the board to the shareholders may be decided by the shareholders anytime after the matter has been referred without notice or compliance with any other internal formalities, except to the extent that the MOI provides otherwise, provided that
  - every such person was present at the board meeting when the matter was referred to them in their capacity as shareholders
  - sufficient persons were present in their capacities as shareholder to satisfy quorum requirements
  - a resolution adopted by those persons in their capacity as shareholders has at least the support that would be required for it to be adopted as an ordinary or special resolution at a properly constituted meeting.

(Note, if these requirements are not satisfied a properly constituted shareholders meeting will have to be held).

2. SEC 58 – Shareholders right to be represented by proxy

2.1 A shareholder may appoint an individual as a proxy to

* participate in, speak and vote at a shareholders meeting
* give or withhold written consent when shareholders consent is sought outside of a meeting of shareholders.

NOTE (a): A proxy appointment

* can be made at any time
* must be in writing, dated and signed by the shareholder
* will be valid for one year ***or*** a longer or shorter time expressly stated in the proxy.

NOTE (b): Except to the extent the MOI provides otherwise

* a shareholder may appoint two or more proxies concurrently, and may appoint different proxies to vote in respect of different securities held by the shareholder

* a proxy may delegate the authority to act to another person (not necessarily a shareholder) subject to any restrictions set out in the document appointing the shareholder
* a copy of the document appointing the proxy must be delivered to the company ***before*** the proxy can exercise the shareholder's rights at a meeting of shareholders.

NOTE (c): An individual appointed as a proxy need ***not*** be a shareholder.

3. SEC 59 – Record date for determining shareholder rights

3.1 The board must set the record date. This is the date which is set to determine which shareholders are entitled to receive notice of the shareholders meeting, participate and vote in the meeting, receive a distribution (e.g. dividend).

NOTE (a): Shareholders in listed companies change frequently so it is important to establish this "cut-off" date.

4. SEC 60 – Shareholders acting other than at meetings

4.1 A resolution which could be voted on at a shareholders meeting may instead be
* submitted to the shareholders for consideration and
* voted on in writing by the shareholders.

NOTE (a): The resolution must be voted on within 20 business days of the submission of the resolution to the shareholders.

NOTE (b): The resolution will have the same voting requirements for adoption as if it had been proposed at a meeting (e.g. ordinary resolution, special resolution), and if adopted, will have the same effect as if it had been approved by voting at a meeting.

NOTE (c): The election of a director may also be conducted by written polling.

NOTE (d): The results of any written polling, and the adoption of any resolution not voted on at a meeting must be communicated to every shareholder who was entitled to vote within 10 business days.

NOTE (e): Any business of a company that must be conducted at an annual general meeting in terms of the MOI or the Act, ***cannot*** be conducted by written polling.

5. SEC 61 – Shareholders meetings

5.1 The board of a company, or any person specified in the MOI or rules, ***may*** call a shareholders meeting at any time.

5.2 Subject to Sec 60, the company ***must*** hold a shareholders meeting
* at any time that the board is required by the Act or the MOI to refer a matter to the shareholders for decision
* whenever required to fill a vacancy on the board
* when otherwise required to by the MOI
* when the annual general meeting of a ***public*** company is required.

NOTE (a): The company ***must*** also call a shareholders meeting if one or more written and signed demands for a meeting are received from shareholders holding at least 10% of the shares entitled to vote on the proposal for which the demand is lodged. The demand must describe the specific purpose for the meeting and "frivolous or vexatious" demands can be set aside by the court on the application of the company or a shareholder. The MOI can set the required percentage at less than 10% (but not more).

5.3 A public company ***must*** convene an annual general meeting. This meeting must be convened, initially no more than 18 months after date of incorporation, and thereafter once in a calendar year but no more than 15 months after the date of the previous AGM.

NOTE (b): The AGM of a public company ***must*** at a minimum, provide for the following business to be transacted

* ***presentation of***
  - the directors' report
  - audited financial statements
  - an audit committee report
* ***election of directors to the extent required by the Act or the MOI***
* ***appointment of***
  - an auditor
  - an audit committee
* ***any matters raised by shareholders*** (with or without advance notice to the company).

NOTE (c): Except to the extent that the MOI provides otherwise

* the board may determine the location of any shareholders meeting
* any shareholders meeting may be held in the Republic or in a foreign country.

NOTE (d): Every shareholders' meeting of a public company must be reasonably accessible within the Republic for electronic participation by shareholders (see Sec 63) irrespective of whether the meeting is held in the Republic or elsewhere.

6. SEC 62 – Notice of meeting

6.1 A ***public*** company (or a non-profit company) must deliver to each shareholder, notice of a shareholders meeting, 15 business days before the meeting is to begin. For all other companies, the notice must be delivered 10 business days before the meeting is to begin.

NOTE (a): The MOI can provide for ***longer*** or ***shorter*** minimum periods.

6.2 The notice of the meeting must include

* date, time and location and record date ("cut-off" date for shareholders)
* general purpose of the meeting and any specific purpose for which the meeting has been demanded by a shareholder where applicable
* a copy of any proposed resolution of which the company has received notice ***and*** a notice of the percentage of voting rights (e.g. ordinary or special) which will be required to adopt the resolution
* a reasonably prominent statement that
  - a shareholder may appoint a proxy (or two or more proxies if the MOI permits)
  - the proxy need not be a shareholder
  - it is a requirement of the Act that personal identification (by shareholders/proxies) is required
* notice that the meeting provides for electronic communication, if applicable. (See Sec 63).

NOTE (b): In addition, the notice of an AGM must include the annual financial statements or a summarized form thereof to be presented and instructions for obtaining a copy of the complete annual financial statements for the preceding year.

NOTE (c): A company may call a meeting with less notice than the prescribed period (15 or 10 business days) or the period stipulated in the MOI. However, for this meeting to proceed, every person who is entitled to exercise voting rights in respect of any item on the agenda must

* be present at the meeting and
* must vote to waive the required minimum notice for the meeting.

7. SEC 63 – Conduct of meetings

7.1 Before a person may attend and participate in a shareholders meeting
* that person must present "reasonably satisfactory identification"
* the person presiding at the meeting must be reasonably satisfied that the right of the shareholder (or proxy) to participate and vote, has been verified.

7.2 Unless prohibited by the MOI, a company may provide for
* a shareholders meeting to be conducted entirely by electronic communication ***or***
* one or more shareholders (proxies) to participate by electronic communication provided the method of electronic communication enables all persons participating in the meeting to do so reasonably effectively and to communicate concurrently, directly with each other.

7.3 Voting on any matter will be done by ***show of hands*** or ***polling*** those present and entitled to vote. On a show of hands, each shareholder will have one vote only irrespective of the number of shares held, but on a poll the shareholder is entitled to exercise all his voting rights.

NOTE (a): If at least 5 persons having the right to vote on a matter or a person or persons holding at least 10% of the voting rights entitled to be voted on that matter, demand that a vote be polled and ***not voted on by show of hands,*** then voting must be by poll.

8. SEC 64 – Meeting quorum and adjournment

8.1 Sec 64 provides for both a ***votes*** quorum and a ***person*** quorum.

8.2 ***Votes quorum***: a shareholders meeting may not begin until persons holding 25% of all the voting rights that can be exercised in respect of at least one matter to be decided at the meeting are present
and
a matter to be decided at the meeting may not begin to be considered unless persons are present at the meeting to exercise at least 25% of all the voting rights that are entitled to be exercised on that matter, at the time the matter is called (dealt with) on the agenda.

8.3 ***Person quorum***: If a company has more than two shareholders, a meeting may not begin, or a matter be debated unless
* at least three shareholders are present
* the ***votes quorum*** is satisfied.

NOTE (a): The MOI may specify a ***lower*** or ***higher*** percentage to replace the 25% in 8.2.

NOTE (b): Remember that different voting rights can attach to different shares. For example, a preference shareholder may only be able to vote on matters affecting preference shares, so a preference shareholder can count towards the quorum to begin the meeting provided there is a matter to be decided pertaining to preference shares, and can count towards the quorum to debate the matter. However, at least 25% of the "preference votes" must be present before the matter affecting the preference shares can be debated.

NOTE (c): If within one hour of the appointed time for the ***meeting to begin***, the quorum requirements (votes and person) are not satisfied, the meeting is postponed without motion (to postpone), vote or further notice, for one week.

NOTE (d): If the quorum requirements to debate a particular matter are not satisfied, the matter may be moved to a later "slot" on the agenda and if at this time the matter is still not quorate, the matter is postponed for one week.

NOTE (e): The MOI may specify a different (longer or shorter) time for the stipulated 1 hour and 1 week.

9. SEC 65 – Shareholders resolutions

9.1 Every resolution of shareholders is either an ***ordinary*** or a ***special*** resolution.

9.2 The board may propose any resolution to be considered by the shareholders, and may determine whether the resolution will be considered at a meeting or by vote or by written consent (no meeting).

9.3 Any two shareholders
* may propose a resolution concerning any matter in respect of which they can exercise votes
* may require that the resolution be considered at
  - a meeting demanded by shareholders
  - the next shareholders meeting or
  - by written vote.

NOTE (a): Proposed resolutions must be expressed with sufficient clarity and specificity and be accompanied by sufficient information to enable a shareholder to decide whether to participate in the meeting and "influence the outcome" of the vote on the resolution.

If a director or shareholder believes that the notice does not satisfy these requirements, he may apply, before the start of the meeting, for a court order restraining the company from putting the resolution to the vote. The court order may also require that the deficiencies in the notice be rectified. Once a resolution has been accepted it ***cannot*** be challenged on the grounds that the notice of the resolution did not comply with the Act.

NOTE (b): For an ***ordinary resolution*** to be approved it must be supported by more than 50% of the voting rights exercised on the resolution.

NOTE (c): The MOI can stipulate a ***higher*** percentage for ordinary resolutions or one or more higher percentages for resolutions relating to different resolutions, e.g. 55% for resolutions relating to capital expenditure, 60% for resolutions relating to investments. (The "more than 50%" requirement for the removal of a director cannot be increased). There must always be at least a difference of 10% between the highest ***ordinary*** resolution percentage and the lowest ***special*** resolution percentage.

NOTE (d): For a ***special resolution*** to be approved, it must be supported by at least 75% of the voting rights exercised on the resolution.

NOTE (e): The MOI can stipulate a different (lower or higher) percentage for a special resolution (or variable higher or lower percentages for different matters) ***but*** at all times there must be a margin of ***at least 10 percent*** between the highest requirements for an ***ordinary*** resolution and the lowest requirement for ***special*** resolution, on any matter.

NOTE (f): A special resolution is required to
* amend the MOI (Sec 16 and 32)
* ratify a consolidated revision of a company's Memorandum of Incorporation (Sec 18)
* ratify actions by the company or directors in excess of their authority (Sec 20)
* approve an issue of shares to a director (Sec 41)
* authorize the granting of financial assistance (Sec 44 and 45)
* approve a decision by the directors to "buy back" shares from a director (Sec 48)

* authorize the basis for compensation to directors (Sec 66)
* approve the voluntary winding up of the company (Sec 80 and 81)
* approve an application to transfer the registration of the company to a foreign jurisdiction (Sec 82)
* approve any fundamental transaction (chapter 5)
  - disposal of all or the greater parts of the assets of the company
  - amalgamations or mergers
  - schemes of arrangement.

NOTE (g): The MOI can stipulate that a special resolution be required to approve matters other than those listed in NOTE (f).

10. SEC 66 – Board, directors and prescribed officers

10.1 The business and affairs of the company must be managed by, or under the direction of, a board of directors.

10.2 The board will have the authority to exercise the powers and perform the function of the company, except to the extent the MOI provides otherwise e.g. the MOI may prohibit the company (and therefore the directors) from acquiring financial derivatives.

10.3 A ***private company*** (and a personal liability company) must have at least ***one*** director.
A ***public company*** must have at least ***three*** directors.

In addition, a public company must appoint an ***audit committee*** and in some cases (e.g. a listed company) a ***social and ethics committee***. The audit committee will require at least 3 independent non-executive directors (Sec 94) in addition to the 3 required to manage the business and affairs of the company. The social and ethics committee must have at least three directors one of which is a non-executive director (not involved in the day to day operations) (Regulation 43). An individual who is independent and non-executive could serve on both committees.

NOTE (a): The MOI may stipulate a ***higher*** minimum number of directors.

NOTE (b): The MOI may provide for
* the direct appointment and removal of one or more directors by any person named in the MOI, e.g. the Chairperson
* a person to be an ***ex officio*** director, e.g. the senior labour relations manager could be an ex officio director by virtue of his status and position in the company. A person, despite holding the relevant office, may not be appointed an ex officio director if he or she becomes ineligible or disqualified to act as a director
* the appointment of alternate directors

but in a ***profit*** company (other than a SOC) the MOI must provide for at least 50% of the directors (and 50% of any alternates) to be elected by the shareholders.

NOTE (c): A person who is ineligible or disqualified from being a director, cannot be elected or appointed as a director (such an appointment will be nullified).

NOTE (d): A director must consent (in writing) to serve as a director.

NOTE (e): The company may pay remuneration to its directors for services as a director except to the extent that the MOI provides otherwise. Remuneration for services as a director may be paid only in accordance with a ***special resolution*** approved by the shareholders within the previous two years.

11. SEC 67 – First director or directors

11.1 Each incorporator of a company is a first director and will serve until sufficient other directors have been appointed.

12. SEC 68 – Election of directors of profit companies (by shareholders)

12.1 ***Each*** director must be:

* elected by the persons entitled to exercise voting rights in the appointment of directors
* to serve for an indefinite term (or a term set out in the MOI)
* voted on separately (as an individual candidate).

12.2 Each voting right can only be exercised once (per candidate) and a majority of voting rights is required.

NOTE (a): Unless the MOI provides otherwise, in any election of directors

* the election is to be conducted as a series of votes, each of which is on the candidacy of a single individual to fill a single vacancy
* each voting right may be exercised once ***per vacancy*** and
* the vacancy is filled only if a majority of the voting rights support the candidate.

Example 1. One vacancy, two candidates, Seb Green, Fred Black.

* voting rights exercised = 100
* votes for Seb Green: 55
* votes for Fred Black: 45

Result: appoint Seb Green

Example 2. One vacancy three candidates, Ben Blue, Rose Red, Joe Grey

* voting rights exercised = 100
* votes for Ben Blue: 35
* votes for Rose Red: 40
* votes for Joe Grey: 25

Result: no appointment (no majority of votes cast). Note: in this situation, Joe Grey would probably be required to withdraw and Ben Blue and Rose Red would contest the vacancy.

13. SEC 69 – Ineligibility and disqualification of persons to be director or prescribed officer

13.1 A person who is ineligible or disqualified ***must not*** be appointed, elected, consent to be, or act as a director.

13.2 A person is ***ineligible*** if the person

* is a juristic person ***or***
* is an unemancipated minor, or under similar legal disability ***or***
* does not satisfy any qualification set out in the MOI.

13.3 A person is ***disqualified*** if the person

* has been prohibited from being a director, or been declared delinquent by a court
* is an unrehabilitated insolvent
* is prohibited in terms of any public regulation from being a director
** has been removed from an office of trust on the grounds of misconduct involving dishonesty ***or***
*** has been convicted in the Republic or elsewhere, and imprisoned without the option of a fine (or fined more than the prescribed amount), for theft, fraud, forgery, perjury or an offence
  - involving fraud, misrepresentation or dishonesty,
  - in connection with the promotion, formation or management of a company or
  - under the Insolvency Act, Companies Act, Close Corporations Act, the Financial Intelligence Centre Act, the Securities Service Act or Chapter 2 of the Prevention and Combating of Corruption Activities Act.

13.4 A director who has been disqualified in terms of ** above (removal from office) or *** above (conviction) will have the disqualification lifted 5 years after the date of removal, or the completion of his sentence. However, the Commission may apply to the court for an extention or extentions of this 5 year period. The court may extend the disqualification

but not for longer than 5 years at a time. The extention is made on the grounds of protecting the public.

13.5 A court may exempt a person from the application of any disqualification in terms of 13.3 above.

13.6 If a director is sequestrated, issued for an order of removal from an office of trust or convicted as in 13.3, the Registrar of the Court must send a copy of the relevant order or particulars of the conviction to the ***Commission***.

13.7 The Commission must in turn, notify each company of which the person is a director.

13.8 The Commission must establish and maintain a ***public register*** of persons disqualified from serving as a director or who are subject to an order of probation as a director.

NOTE (a): The MOI may impose additional grounds for ineligibility or disqualification of directors and/or minimum qualifications to be met by the directors.

14. SEC 71 – Removal of directors

14.1 Despite anything to the contrary in the MOI or rules or any agreement between a company and a director, or between shareholders and a director, a director may be ***removed*** by an ordinary resolution at a shareholders meeting by the persons entitled to exercise voting rights in the ***election*** of that director.

14.2 However, before a director can be removed by the shareholders,
* the director must be given notice of the meeting and the resolution to remove him. The notice period must be at least equivalent to that which a shareholder is entitled to receive, (public company 15 business days notice, 10 business days for other companies, or any longer or shorter notice per the MOI), ***and***
* the director must be afforded a reasonable opportunity to make a presentation (in person or through a representative) to the meeting before voting takes place.

14.3 If a ***shareholder*** or ***director*** alleges that a fellow director has become
* ineligible or disqualified ***or***
* incapacitated to the extent that he cannot perform as a director ***or***
* has neglected or been derelict in his duties as a director

the ***board*** must consider the allegation and may vote on the removal of the director.

NOTE (a): In the situation 14.3 above, where the director is to be removed by the board, the "accused" director may not vote on his removal. He must still be afforded the "notice" and "representation" requirements laid out in 14.2 above.

NOTE (b): A director removed by the board may apply (within 20 business days) to the court for a review. If the director is ***not*** removed, any director or shareholder who voted to have the said director removed, may also apply to the court for a review. Any holder of voting rights which may be exercised in the ***election*** of that director can also apply to the court for a review.

NOTE (c): If a company has ***less than three directors***, this section cannot operate as there would either be no remaining director to vote (one director company) or one remaining director to vote (two director company). In this case, the aggrieved director or shareholder can apply to the Companies Tribunal.

15. SEC 72 – Board committees

15.1 Except to the extent the MOI provides otherwise, the board may
* appoint any number of committees of directors and
* delegate any authority of the board to any committee

15.2 Except to the extent the MOI (or the resolution to appoint a committee) provides otherwise, the committee
* may include persons who are ***not*** directors of the company ***but***
  - such a person must not be ineligible or disqualified from being a director ***and***
  - will not have a vote on any matter to be decided by the committee
* may consult with or receive advice from any person
* has the full authority of the board in respect of a matter referred to it.

NOTE (a): The creation of a committee, delegation of any power to a committee or action taken by a committee, does not alone satisfy or constitute compliance by a director with his duties (standards of conduct) as a director of the company, i.e. the directors (as a board) remain responsible.

NOTE (b): The Minister has prescribed that certain company's appoint a ***social and ethics committee*** (see Regulation 43 below) if it is desirable in the public interest having regard to
- its annual turnover
- the size of its workforce
- the nature and extent of its activities.

Regulation 43
In terms of this regulation, the following companies must appoint a ***social and ethics committee***
* listed public companies
* state owned companies
* any other company that has in any two of the previous 5 years, scored above 500 points in its public interest score.

See the start of this chapter for more information on this regulation (pg 3/10).

16. SEC 73 – Board meetings

16.1 A director authorized by the board e.g. managing director
* ***may*** call a meeting of directors at any time
* ***must*** call a meeting of directors if required to do so by at least
  - 25% of the directors in the case of a company which has at least 12 directors (e.g. 4 of 14 directors)
  - two directors in any other case (e.g. 2 of 9 directors).

NOTE (a): The MOI may specify a ***higher*** or ***lower*** percentage or number.

NOTE (b): Except as to the extent the MOI or Companies Act provides otherwise, a meeting of the board may be conducted by electronic communication or a director(s) may participate electronically, as long as the electronic communication facilitates concurrent and effective communication between directors.

NOTE (c): ***Notice***.
* The board must determine the form and time for giving notice of the meeting in compliance with the MOI,
* notice must be given to all directors.

Quorum
* a majority of the directors must be present before a vote may be called.

Except to the extent that the company's MOI provides otherwise, if all of the directors of the company acknowledge actual receipt of the notice, are present at the meeting, or waive the notice of the meeting, the meeting may proceed even if the required notice period was not given or there was a defect in giving the notice.

Voting
* each director has one vote, and a majority of votes ***cast*** approves a resolution

* in the case of a tied vote, the chair has a casting vote if the chair did not initially have a vote or cast a vote, otherwise the matter being voted on, fails (the chair does not get two votes in the event of a tie).

NOTE (d): The board and its committees must keep minutes which reflect every resolution adopted by the company (and other important discussions etc held at the meeting).

NOTE (e): Resolutions adopted must be dated and sequentially numbered, and become immediately effective unless it is otherwise stated in the resolution. Any minute of a meeting or a resolution signed by the chair of the meeting, or by the chair of the next meeting is evidence of the proceedings of that meeting, or adoption of that resolution.

NOTE (f): The MOI may alter the requirements for directors meetings.

17. SEC 74 – Directors acting other than at meeting

17.1 Except to the extent that the MOI provides otherwise, a resolution which could be voted on at a meeting, can be adopted by "written consent" or by electronic communication provided each director has received notice of the matter to be voted on.

18. SEC 75 – Directors personal financial interests

18.1 The common law situation is that all contracts between a director and the company are voidable at the option of the company. This flows from the principle that there should be no "conflict of interest" between the director and the company. Remember that a director is required to look after the interests of the company and not his own interests. The statutory arrangement presents a means of accommodating this common law principle, but does not replace it.

18.2 If a director has a personal financial interest, or knows that a person related (as defined) to him has a personal financial interest in a matter to be considered at a meeting of the board, that director

* ***must*** disclose the interest and its general nature before the matter is considered at the meeting e.g. the director should disclose a 15% shareholding he has in the company with which the board is considering entering into a contract.
* ***must*** disclose to the meeting, any material information he has relating to the matter e.g. he may be aware that the other company is in financial difficulty (a fact not known to his fellow directors).
* ***may*** disclose any observations/insights if requested to do so by the other directors e.g. his opinion on the extent of the financial difficulties.
* ***must not*** take part in the consideration of the matter (other than as above) and must leave the meeting.

NOTE (a): A director may at any time, notify the company in writing of his financial interests. This will suffice as a general disclosure for the purposes of this section.

NOTE (b): When an "interested" director has left the meeting, he remains part of the quorum, but cannot vote and will not be counted as being present in determining whether the resolution can be adopted.

NOTE (c): If a director (or related person) acquires a personal financial interest in an "agreement/matter" in which the company of which he is a director has an interest ***after*** the "agreement/matter" has been approved, the director must promptly disclose to the board

* the nature and extent of that interest e.g. 15% shareholding, and
* the material circumstances relating to the acquisition of the interest (this is to determine whether there has been any irregular/fraudulent intention on the part of the director to get around declaring his interest ***before*** the contract was approved).

NOTE (d): A contract in which a director (or related person) has a financial interest, will be ***valid***

* if it was approved after full disclosure as in 18.2 above.

If the contract was approved ***without*** the necessary disclosure, the contract will be valid if

* it has been subsequently ratified by an ordinary resolution (interest must be disclosed)
* it has been declared to be valid by a court (any interested party can apply to the court).

NOTE (e): If the director does not declare his interest, any interested party can apply to the court to have the contract declared valid. However, if neither NOTE (d) or (e) applies, the contract is voidable at the option of the company.

NOTE (f): There are a number of exclusions to this section. The section will ***not*** apply to

* a director or a company if one person holds all the issued securities (shares) ***and*** is the only director. Effectively there is no real "conflict of interest" as the company and the individual are one and the same
* a director in respect of a decision which may generally affect all directors in their capacity as directors e.g. decision on directors' bonuses
* a decision to remove the director from office.

NOTE (g): If a director who has a financial interest is the sole director ***but*** does not hold all the issued securities (shares) in the company, the said director cannot approve the agreement:

* it must be approved by ordinary resolution of the shareholders
* after the director has disclosed the nature and extent of his interest to the shareholders.

NOTE (h): For the purposes of this section, the term director includes

* an alternate director
* a prescribed officer
* a person who is a member of a committee of the board, irrespective of whether or not the person is also a member of the company's board. (Note that a person who is not a member of the board may be appointed to a board committee but will not have a vote on the committee.)

19. SEC 76 – Standards of directors conduct

19.1 A director of a company must

* ***not use the position of director***, or any information obtained whilst acting as a director
  - to gain an advantage for himself or any other person other than the company (or its wholly owned subsidiary) ***or***
  - knowingly cause harm to the company (or a subsidiary of the company)
* ***communicate to the board*** at the earliest practicable opportunity, any information that comes to his attention, ***unless*** he reasonably believes that the information is
  - immaterial to the company ***or***
  - generally available to the public or known to the directors ***or*** unless
  - he is bound not to disclose that information by a legal or ethical obligation of confidentiality
* ***exercise the powers and functions of director***
  - in good faith and for a proper purpose
  - in the best interests of the company
  - with the degree of care, skill and diligence reasonably expected of a director.

NOTE (a): To ensure that he has exercised his powers and functions in compliance with the above, a director

* should take reasonably diligent steps to be informed about any matter to be dealt with by the directors
* should have had a rational basis for making a decision and believing that the decision was in the best interests of the company
* is entitled to rely on the performance of
  - employees of the company whom the director reasonably believes to be reliable and competent
  - legal council, accountants or other professionals retained by the company
  - any person to whom the board may have reasonably delegated authority to perform a board function
  - a committee of the board of which the director is not a member, unless the director has reason to believe that the actions of the committee do not merit confidence
* is entitled to rely on information, reports, opinions recommendations made by the above mentioned persons.

NOTE (b): For the purposes of this section, the term director includes
* an alternate director
* a prescribed officer
* a person who is a member of a committee of the board, irrespective of whether or not the person is also a member of the company's board. Note that a person who is not a member of the board may be appointed to a board committee but will not have a vote on the committee.

20. SEC 77 – Liability of directors and prescribed officers

20.1 A director may be held liable
* in terms of the common law for a ***breach of fiduciary duty*** for any loss, damages or costs sustained by the company as a consequence of any breach by the director of his duty to the company
  - failing to disclose a personal financial interest (Sec 75)
  - using the position of director to gain advantage for himself or harm the company (Sec 76)
  - failing to act in good faith and for a proper purpose
  - failing to act in the best interests of the company
* in terms of the common law ***relating to delict*** for any loss, damages or costs sustained by the company as a result of any ***breach*** of the director of
  - the duty to act with the necessary degree of care, skill and diligence
  - any provision of the Act not specifically mentioned in section 77
  - any provision of the Memorandum of Incorporation.

20.2 A director may be held liable to the company for any loss, damage or costs arising as a direct or indirect consequence of the director
* acting for the company despite knowing that he lacked authority
* agreeing to carry on business knowing that to do so was "reckless" (Sec 22)
* being party to an act or omission despite knowing that it was calculated to defraud a creditor, employee or shareholder, or that the act or omission had another fraudulent purpose
* having signed, or consented to the publication of a document e.g. financial statements, prospectus, which was false, misleading or untrue, despite knowing the publication to be so
* being present at a meeting, or participating in the taking of a decision and failing to vote against
  - the issuing of unauthorized shares, securities or the granting of options, whilst knowing the shares, securities or options were not authorized (Sec 36, 42)
  - the issuing of authorized shares, despite knowing that the issue was inconsistent with the Act (Sec 41)
  - the provision of financial assistance to any person including a director (as defined) whilst knowing that the financial assistance was in contravention of the Act or MOI

- a resolution approving a distribution (as defined) whilst knowing the distribution was in contradiction of the Act (Sec 46). (Only applies if liquidity/solvency test is not satisfied, and it was unreasonable at the time to think the test would be satisfied.)
- the acquisition by a company of its own shares, whilst knowing that the acquisition was contrary to the Act (Sec 46, 48)
- an allotment (of securities) whilst knowing that the allotment was contrary to the Act.

NOTE (a): In addition, each shareholder has the right to claim damages from any director who fraudulently or due to gross negligence, causes the company to do anything inconsistent with the Act.

NOTE (b): The MOI and rules will be binding between each director (prescribed officer) and the company.

NOTE (c): For the purposes of this section, the term "director" includes
* an alternate director
* a prescribed officer
* a person who is a member of a board committee, irrespective of whether or not the person is also a member of the board. Note that a person who is not a director may be appointed to a board committee but will not have a vote on this committee.

NOTE (d): The liability of a director in terms of this section will be joint and several with any other person who is held liable for the same act.

21. SEC 78 – Indemnification and directors insurance

21.1 Any provision of an agreement, the MOI or rules, or a resolution of a company, is ***void*** if it directly or indirectly seeks to relieve a director of any of that director's ***duties*** in respect of
* personal financial interests (Sec 75) or
* the standards of directors conduct (Sec 76) or
* liability arising from Sec 77 (e.g. fiduciary duty, breach of good faith, any provisions of the Act or MOI).

21.2 Any provision, rule, the MOI or resolution which seeks to limit, negate, or limit any legal consequence from an act or omission which constitutes wilful misconduct or wilful breach of trust, will also be void.

21.3 A company may not directly or indirectly pay any fine that may be imposed on a director of the company (or a related company) who has been convicted of an offence.

21.4 Except to the extent that the MOI provides otherwise, a company may advance expenses to a director to defend litigation in any proceedings arising out of the director's service to the company.

21.5 Except to the extent that the MOI provides otherwise, a company may ***indemnify*** (protect) a director in respect of any liability ***except*** where the director:
* acted in the name of the company despite knowing he lacked the authority to do so ***or***
* acquiesced (agreed without protest) in the carrying on of the business recklessly, with gross negligence, with intent to defraud any person or to trading under insolvent circumstances ***or***
* was a party to an act or omission intended to defraud a creditor, employee or shareholder ***or***
* committed wilful misconduct or wilful breach of trust.

The company may not indemnify the director against any fine suffered by the director in respect of the above 4 situations.

NOTE (a): The wider definition of director applies to Sec 78, i.e. prescribed officer, a member of a board committee and also includes a former director.

NOTE (b): The prohibition in 21.3 does not apply to a private company if
* a single individual is the sole shareholder and sole director of the company
* two or more related individuals are the only shareholders and there are no directors, other than one or more of the related individuals,

CHAPTER 2 - Part G – Winding up of solvent companies and deregistering companies. This part is beyond the scope of this text.

CHAPTER 3 – ENHANCED ACCOUNTABILITY AND TRANSPARENCY

CHAPTER 3 – Part A – Application and general requirement of this chapter

1. SEC 84 – Application of chapter

1.1 The requirements of this chapter apply to
- * public companies
- * state owned companies (subject to exemptions in Sec 9)
- * a private company, personal liability company or a non-profit company
  - if the company is required by the Act or Regulations to have its AFS ***audited*** every year e.g. a private company with a public interest score which is at least 350. However Parts B (company secretary) and D (audit committees) will not apply to these companies
- * a private company, personal liability company or a non-profit company (not required to be audited) but only to the extent required by the company's MOI.

1.2 The requirements of the chapter hinge around the appointment of
- * a company secretary PART B
- * an external auditor PART C
- * an audit committee PART D

The intention of the section is to enhance the accountability and transparency of the company.

NOTE (a): ***Any person who is disqualified from acting as a director of a company may not be appointed as company secretary, auditor or to the audit committee of that company.***

2. SEC 85 – Registration of company secretary and auditor

2.1 Every company (public, state-owned, private etc) which appoints a company secretary or auditor whether ***in terms of the act, regulations or voluntarily***
- * must maintain a record of its company secretary and auditor
  - name of person
  - date of appointment
- * if a firm or juristic person is appointed
  - name, registration and registered office address of the firm or juristic person
  - the name of the "designated auditor" i.e. the individual who takes responsibility for the audit. (Sec 44 Auditing Profession Act 2005).

NOTE (a): Within 10 business days of making an appointment of the above, or after the termination of such appointment, the company must file notice of the appointment or termination. All changes must be recorded.

CHAPTER 3 - Part B – Company Secretary

1. SEC 86 – Mandatory appointment of secretary

1.1 A public company or state-owned company ***must*** appoint a company secretary.

NOTE (a): The company secretary must be resident in the Republic and must remain so while serving in that capacity (this will also be the case for voluntary appointments of a company secretary e.g. by a private company in terms of Sec 34(2)).
The only other requirement is that the company secretary has "the requisite knowledge of, and experience in, relevant laws. But don't forget that a person who is disqualified from acting as a director is also disqualified from being appointed company secretary.

NOTE (b): The first company secretary of a public or state owned company may be appointed by
* the incorporators of the company or
* within 40 business days after incorporation by
  - either the directors or
  - an ordinary resolution of the shareholders.

NOTE (c): Within 60 business days after a vacancy in the office of company secretary arises, the ***board*** must fill the vacancy by appointing a person who has the "requisite knowledge and experience" – no formal qualification or membership of a professional body required!

2. SEC 87 – Juristic person or partnership may be appointed company secretary

2.1 A juristic person or partnership may be appointed company secretary provided
* no employee of the juristic person, or partner and employee of that partnership is disqualified from acting as a director of that company and
* at least one of the employees (or partners) is
  - resident in the Republic and
  - has the requisite knowledge of and experience in relevant laws.

NOTE (a): A change in the membership/partners/employees of the juristic person or partnership holding the appointment of company secretary, does not constitute a casual vacancy if the juristic person or partnership continues to satisfy the requirements as indicated in 2.1 above. If circumstances change and the juristic person/partnership no longer satisfies the basic requirements of 2.1, it must notify the company. A vacancy will then have arisen.

3. SEC 88 – Duties of company secretary

3.1 The company secretary is accountable to the company's board and the company secretary's duties include
* providing the directors of the company with guidance as to their duties, responsibilities and powers
* making the directors aware of any law relevant to the company
* reporting to the board on any failure on the part of the company or a director to comply with the Act or MOI
* ensuring that minutes of all meetings of
  - shareholders
  - directors
  - board committees including
  - the audit committee, are properly recorded
* certifying in the company's annual financial statements, that the company has filed the necessary returns and notices in terms of this Act, and whether all such returns and notices appear to be true, correct and up to date
* ensuring that a copy of the annual financial statements is sent to every person who is entitled to receive it.

4. SEC 89 - Resignation or removal of company secretary

4.1 A company secretary may ***resign*** by giving
* one months written notice or
* less than one month with the approval of the board.

4.2 If the company secretary is ***removed*** from office, he may require the company to include a statement of reasonable length in the annual financial statements, setting out the secretary's "opinion" on the circumstances which resulted in his removal. This statement will appear in the directors' report.

CHAPTER 3 - Part C – Auditors

1. SEC 90 - Appointment of auditor

1.1 ***Public*** companies and ***state-owned companies must*** appoint an auditor at the annual general meeting.

If a ***private*** (or any other company) is required by the Act or Regulations to have its financial statements audited, e.g. it has a public interest score of 350 points or more, the appointment of the auditor must take place at the AGM at which the requirement first applies, and at every AGM thereafter.

1.2 To be appointed as auditor, an individual or firm

* ***must be***
  - a registered auditor (IRBA)
* ***must not be***
  - a director or prescribed officer of the company
  - an employee or consultant of the company who was or has been engaged for more than one year in the maintenance of any company's financial records or preparation of any of its financial records
  - a director, officer or employee of a person appointed as company secretary
  - a person who alone or with a partner or employee, habitually or regularly performs the duties of accountant or bookkeeper, or performs related secretarial work for the company
  - a person who at any time during the five financial years immediately preceding the date of appointment, was a person contemplated in any of the four categories above, e.g. must not have been a director for any period during the preceding five years
  - a person related (as defined) to a person contemplated in the five categories above.

NOTE (a): The person appointed as auditor must be acceptable to the company's audit committee (public companies and state owned companies must appoint an audit committee) as being ***independent*** of the company. To do this, the audit committee must

* ascertain that the auditor does not receive any direct or indirect remuneration or other benefit from the company except
  - as auditor or
  - for rendering other non-audit services which have been determined by the audit committee
* consider whether the auditor's independence may have been prejudiced
  - as a result of any previous appointment as auditor or
  - having regard to the extent of any consultancy, advisory or other work undertaken by the auditor for the company and
* consider whether the auditor complies with the "rules and regulations" of the Independent Regulatory Board (IRBA) e.g. the Code of Professional Conduct, in relation to independence and conflict of interest.

The audit committee must evaluate the independence of the auditor in the context of the company itself, and within the group of companies if the company is a member of a group.

NOTE (b): Any person who is disqualified from serving as a director of the company is also disqualified from being the auditor of the company.

NOTE (c): Where a firm is appointed as auditor, the person designated as the auditor to be responsible for the audit function, must satisfy the above requirements.

NOTE (d): A retiring auditor (i.e. an auditor coming to the end of the annual appointment) may be automatically re-appointed without a resolution being passed at the AGM unless:

* the retiring auditor is
  - no longer qualified for appointment
  - no longer willing to accept the appointment, and has notified the company
  - required to be "rotated" in terms of the Act (Sec 92)
* the audit committee objects to the re-appointment ***or***
* the company has notice of an intended resolution to appoint some other person/firm as auditor.

NOTE (e): If an annual general meeting of a company does not appoint/reappoint the auditor, the directors must fill the vacancy within 40 business days.

2. SEC 91 – Resignation of auditors and vacancies

2.1 The resignation of an auditor is effective when the notice (of resignation) is filed with the Commission.

2.2 The procedure to be followed where a vacancy arises, is as follows
* the board must propose to the audit committee, within 15 business days, the name of at least one registered auditor to be considered for appointment
* the audit committee has 5 business days after the proposal is delivered to it, to ***reject*** the proposed replacement auditor in writing, if they so wish, otherwise the board may make the appointment
* whatever the situation, a new auditor must be appointed within 40 business days of the vacancy arising.

NOTE (a): If the company has appointed a firm as auditor, a change in the composition of the members (partners/shareholders) of the firm, does not create a vacancy in the office of auditor unless ***less*** than half of the audit firm members remain. If this situation (less than half remain) does arise, it will constitute a resignation of the auditor and a vacancy will have arisen.

NOTE (b): If there is no audit committee the board will make the appointment.

3. SEC 92 – Rotation of auditors

3.1 The same individual may not serve as auditor (or designated auditor in the case of a firm holding the appointment) of a company for more than ***5 consecutive years***.

3.2 If an individual has served as auditor (or designated auditor) for two or more consecutive financial years and then ceases to be the auditor, the individual may not be appointed again as auditor (designated auditor) of that company until the expiry of at least two further financial years, e.g. Jake Blake was the designated auditor of Craneworks Ltd for the financial year-ends 31 December 0001 and 0002. In 0003 he resigned from the audit firm but returned in January 0004; he cannot be appointed as the auditor of Craneworks Ltd until ***after*** the financial year-end 0004. There appears to be nothing to prevent him from being part of the audit team however.

NOTE (a): If a company (e.g. a bank) has appointed joint auditors, the rotation must be managed so that both joint auditors do not relinquish office in the same year (i.e. there must be continuity).

4. SEC 93 – Rights and restricted functions of auditors

4.1 The auditor of a company has the right of access at all times, to the accounting records and all books and documents of the company and is entitled to require from the directors (or prescribed officers) information and explanations necessary for the performance of his duties.

4.2 The auditor of a holding company, who is not the auditor of the holding company's subsidiary company(ies) has right of access to all current and former financial statements of the subsidiary(ies) and is entitled to require from the directors (or prescribed officers) of the holding company ***and*** the subsidiary, any information and explanations in

connection with any such statements and accounting records, books and documents of the subsidiary as necessary for the performance of his duties.

4.3 The auditor is entitled to
* attend any general shareholder meeting (including AGM)
* receive all notices of, and other communications relating to, any general shareholders meeting
* be heard at any general shareholders meeting on any part of the business of the meeting that concerns the auditor's duties or functions.

NOTE (a): If an auditor does not have "access", the audit function cannot be carried out. Access enables the auditor to be independent.

NOTE (b): An auditor may apply to a court for an appropriate order to enforce his rights. The court may make any order (with costs) that is just and reasonable to prevent ***frustration of the auditor's duties by the company, directors, prescribed officers or employees***. The court may also make an order of costs personally against any director or prescribed officer whom the court has found to have wilfully and knowingly frustrated or attempted to frustrate the performance of the auditor's functions.

CHAPTER 3 - Part D – Audit committees

1. SEC 94 – Audit committees

1.1 At each annual general meeting, a public company or state owned company (or any other company that has voluntarily decided in terms of its MOI to have an audit committee) must elect an audit committee comprising at least ***three*** members, unless
* the company is a subsidiary of another company that has an audit committee ***and***
* the audit committee of that company will perform the functions of the audit committee on behalf of that subsidiary.

1.2 Each member of an audit committee
* ***must***
  - be a director of the company and
  - satisfy any minimum qualifications the Minister may prescribe to ensure that the audit committee taken as a whole, comprises persons with adequate financial knowledge and experience (see Note (a) below).
* ***must not be***
  - involved in the day to day management of the company's business or have been involved at any time during the previous financial year ***or***
  - a prescribed officer, or full-time executive employee of the company or another related or inter-related company, or have held such a post at any time during the previous three financial years ***or***
  - a material supplier or customer of the company, such that a reasonable and informed third party would conclude that in the circumstances, the integrity, impartiality or objectivity of that member of the audit committee would be compromised
  - a "related person" to any person subject to the above prohibitions.

NOTE (a): ***Regulation 42*** requires that at least one third of the members of a company's audit committee must have academic qualifications, or experience in economics, law, accounting, commerce, industry, public affairs, human resources or corporate governance.

NOTE (b): Any vacancy on the audit committee must be filled by the board within 40 business days.

NOTE (c): The duties of an audit committee are to

* nominate for appointment as auditor of the company, a registered auditor who, in the opinion of the audit committee, is independent of the company.
* determine the fees to be paid to the auditor and the auditor's terms of engagement.
* ensure that the appointment of the auditor complies with the provisions of this Act, and any other legislation relating to the appointment of auditors.
* determine the nature and extent of any non-audit services that the auditor may provide to the company, or that the auditor must not provide to the company, or a related company.
* pre-approve any proposed agreement with the auditor for the provision of non-audit services to the company.
* prepare a report to be included in the annual financial statements for that financial year
  - describing how the audit committee carried out its functions
  - stating whether the audit committee is satisfied that the auditor was independent of the company; and
  - commenting in any way the committee considers appropriate on the financial statements, the accounting practices and the internal financial control of the company.
* receive and deal appropriately with any concerns or complaints, whether from within or outside the company, or on its own initiative, relating to
  - the accounting practices and internal audit of the company.
  - the content or auditing of the company's financial statements.
  - the internal financial controls of the company; or
  - any related matter.
* make submissions to the board on any matter concerning the company's accounting policies, financial control, records and reporting; and
* perform such other oversight functions as determined by the board.

CHAPTER 4 – PUBLIC OFFERINGS OF COMPANY SECURITIES

The offering of securities in a company to the public is governed by Chapter 4 of the Companies Act 2008. The offering of shares is regarded as specialist knowledge by both the IRBA and SAICA and is therefore not covered by this text.

CHAPTER 5– FUNDAMENTAL TRANSACTIONS,TAKEOVERS AND OFFERS

This chapter identifies three fundamental transactions namely:

* the disposal of all or the greater part of the assets or undertaking of a company
* amalgamations or mergers
* schemes of arrangement

As the implementation of any of these transactions is by definition, fundamental to the ongoing state of the company, strict requirements are laid down for their approval.

Again, takeovers, mergers, amalgamations, schemes of arrangement are expected to be regarded as specialist knowledge from an audit perspective and thus are not covered in any detail in this text. However, it has been decided to include a brief summary of the approval requirements to supplement the financial accounting knowledge which students will gain through their accounting studies.

CHAPTER 5 - Part A – Approval for certain fundamental transactions

1. SEC 112 –Proposals to dispose of all or greater part of assets or undertaking.

1.1 A company may ***not*** dispose of all or the greater part of its assets or undertaking unless
* the disposal has been approved by a ***special resolution*** of the shareholders
* notice of the meeting to pass the resolution is delivered in the prescribed manner within the prescribed time and
* the notice includes a written summary of the terms of the transaction and the provisions of Sec 115 and 164. (Sec 164 deals with the rights of dissenting shareholders).

NOTE (a): In terms of Sec 115, the special resolution must be
i. adopted by persons entitled to exercise voting rights on the matter,
ii. at a meeting called for the purpose of voting on the proposal and
iii. at which sufficient persons are present to exercise, in aggregate, at least 25% of all of the voting rights that are entitled to be exercised on that matter.

NOTE (b): If the company proposing the sale (of its assets etc) is a subsidiary company ***and*** the sale will also constitute the disposal of the greater part of the holding company's assets or undertaking, a special resolution must be obtained from the holding company shareholders.

NOTE (c): Neither the Memorandum of Incorporation, nor the resolution taken by the Board or the shareholders, can override the approval requirements of Sec 112 and 115.

NOTE (d): The requirements of Sec 112 and 115 will not apply to a proposal to dispose of all or the greater part of the assets or undertaking if the disposal would constitute a transaction
i. pursuant to a business rescue plan
ii. between a wholly owned subsidiary and its holding company
iii. between or among
* two or more wholly owned subsidiaries of the same holding company or
* a wholly owned subsidiary and its holding company and other wholly owned subsidiaries of that holding company.

2. SEC 113 – Proposals for amalgamation or merger

2.1 Two or more companies proposing to amalgamate or merge, must enter into a written agreement which sets out:
* the proposed Memorandum of Incorporation of any new company to be formed.
* the name and identity of each proposed director of any new company to be formed.
* the manner in which securities in the merging companies will be converted into securities of any new company to be formed.
* the consideration (and method of payment) which holders of securities of the merging companies will receive where those securities are not being converted into securities of any new company to be formed.
* details of the proposed allocation of assets and liabilities of the merging companies to any new companies to be formed or which will continue to exist.
* details of any arrangement or strategy to complete the merger and the subsequent management and operation of the new entity.
* the estimated cost of the proposed amalgamation or merger.

NOTE (a): Two or more profit companies may amalgamate or merge if upon amalgamation or merging, each amalgamation or merged company will satisfy the ***solvency/liquidity*** test.

NOTE (b): In terms of Sec 115, a proposed merger (amalgamation) must be approved
i. by a special resolution

ii. adopted by persons entitled to exercise voting rights in respect of such a matter,
iii. at a meeting called for the purpose of voting on the proposal and
iv. at which sufficient persons are present to exercise, in aggregate at least 25% of all the voting rights that are entitled to be exercised on that matter.

NOTE (c): The notice of the meeting at which the proposal will be considered, must be sent to each shareholder of all of the companies proposing to merge and must contain a copy of the
i. merger (amalgamation) agreement
ii. a summary of the requirements of Sec 115 and 164 (Sec 164 deals with the rights of dissenting shareholders)

NOTE (d): Neither the Memorandum of Incorporation nor any resolution of the Board or the shareholders can override the approval requirements of Sec 114 and 115.

3. SEC 114 – Proposals for scheme of arrangement

3.1 The board of a company may propose (and implement if approval is granted) an arrangement between the company and its security holders to
i. consolidate securities of different classes
ii. divide securities into different classes
iii. expropriate or re-acquire securities from the holders
iv. exchange any of its securities for other securities or
v. implement a combination of the above (i to iv).

3.2 Any Board proposing such a scheme must engage an ***independent*** expert to prepare a report to the Board which must as a minimum
i. state all information relevant to the value of the securities affected by the proposed arrangement
ii. identify every type and class of holders of securities affected by the proposed arrangement
iii. describe the material effects that the arrangement will have on the holders of these securities
iv. evaluate the adverse effects of the arrangement on the rights and interests of holders against
- any compensation received by holders and
- any reasonably probable benefits to be derived by the company

v. state any material interest of any director of the company or trustee for security holders and state the effect of the arrangement on those interests.
vi. include a copy (or summary) of Sec 115 and 164 (Sec 164 deals with the rights of dissenting shareholders).

NOTE (a): In terms of Sec 115, such a scheme of arrangement must be approved by special resolution.

NOTE (b): The expert engaged by the company ***must*** be
* qualified and have the competence and experience to
  - understand the type of arrangement proposed
  - evaluate the consequences of the arrangement and
  - assess the effect of the proposed arrangement on the value of securities and on the rights and interests of a holder of any securities, or the creditor of the company.
* able to express opinions, exercise judgment and make decisions impartially.

NOTE (c): The expert engaged ***must not***
* have any relationship with the company which would lead a reasonable and informed third party to conclude that the integrity, impartiality or objectivity of the expert is compromised by that relationship.
* have had any such relationship within the immediately preceding two years or

* be related to any person who has or has had such a relationship.

NOTE (d): Neither the Memorandum of Incorporation nor any resolution of the board or security holders, can override the requirements of Sec 113 or 115 in respect of a scheme of arrangement.

CHAPTER 5 - Part B – Authority of Panel and Takeover Regulations – nil

CHAPTER 5 - Part C – Regulation of affected transactions and offers – nil

CHAPTER 6 – BUSINESS RESCUE AND COMPROMISE WITH CREDITORS

For the purposes of students following the IRBA and SAICA qualifying syllabuses, this chapter is expected to be regarded as specialist knowledge. However, "business rescue" is linked to the going concern ability of a company and it has therefore been decided that this text should provide students with an understanding of the basics underlying the chapter.

CHAPTER 6 - Part A - Business rescue proceedings

1. SEC 128** – **Definitions (selected)

1.1 ***Business rescue*** means proceedings to facilitate the rehabilitation of a company that is financially distressed by providing for
   i. the temporary supervision of the company, and of the management of its affairs, business and property
   ii. a temporary moratorium on the rights of claimants against the company or in respect of property in its possession (e.g. attaching an asset given as security for a loan) and
   iii. the development and implementation (if approved) of a plan to rescue the company, re-structuring its affairs, business, property, debt, equity etc.

1.2 ***Financially distressed*** means that

   i. it appears to be reasonably unlikely that the company will be able to pay all of its debts as they fall due and payable within the immediately ensuing six months or
   ii. it appears to be reasonably likely that the company will become insolvent within the immediately ensuing six months.

1.3 ***An affected person*** means

   i. a shareholder or creditor of the company
   ii. any registered trade union representing employees of the company
   iii. any employee(s) not represented by a trade union.

1.4 ***Business rescue practitioner*** means a person(s) appointed to oversee the company during rescue.

NOTE (a): A business rescue practitioner must be licenced with the Commission and the Minister may prescribe qualifications (see Regulation 126) to practice as a business rescue practitioner. The Commission has a right to revoke the licence.

Regulation 126.
For the purposes of business rescue, this regulation categorises companies (basically in terms of their public interest score) ***and*** business rescue practitioners in terms of their experience. This is done to identify which practitioners can be appointed to "rescue" which companies. The categorizations are as follows:

Company	Score	Practitioner	Experience
Large	500 or more	Senior	Member of accredited professional body, e.g. SAICA. At least ten years business turnaround/rescue experience.
Medium	Public: less than 500 Other: 100 to 499	Experienced	Member of accredited professional body e.g. SAICA. At least five years business turnaround/rescue experience.
Small	Less than 100	Junior	Member of accredited professional body e.g. SAICA but less than five years experience or no experience at all.

Note: The regulations do not include state owned companies in the categorization.

(i) A ***senior*** practitioner may be appointed as a practitioner for any company.
(ii) An ***experienced*** practitioner may be appointed as a practitioner for any ***small*** or ***medium*** company but ***not*** for a ***large*** company or ***state owned*** company unless as an assistant to a senior practitioner.
(iii) A ***junior*** practitioner may be appointed as a practitioner for any ***small*** company but ***not*** for a ***large*** or ***medium*** company or for a state owned company unless as an assistant to a senior or experienced practitioner.

2. SEC 129 – Company resolution to begin business rescue proceedings

2.1 The Board may resolve that the company commence business rescue proceedings if the board has reasonable grounds to believe that
* the company is financially distressed ***and***
* there appears to be a reasonable prospect that the company can be rescued.

If liquidation proceedings have been initiated by or against the company, such a resolution may not be adopted.

2.2 The resolution must be filed with the Commission.

2.3 Thereafter the company must
i. publish a notice of the resolution to every affected person within 5 business days of filing,
ii. appoint a ***business rescue practitioner*** within 5 business days of filing,
iii. file the name of the business rescue practitioner (with the Commission) within 2 business days of appointment, and within 5 business days of that appointment, notify all affected persons of the notice of appointment.

NOTE (a): In terms of Sec 138, a person may be appointed as a practitioner only if the person is
i. a member in good standing, of a profession which is regulated (such as SAICA or IRBA)
ii. not disqualified from acting as a director of the company or subject to an order of probation
iii. does not have any relationship with the company which would lead a reasonable and informed third party to conclude that the integrity, impartiality or objectivity of that person is compromised by that relationship
iv. is not related to a person who has a relationship contemplated in (iii) above.

NOTE (b): In terms of Sec 130, an affected person can apply to the court at any time after the adoption of the rescue resolution but before the adoption of the rescue plan (Sec 150) to
i. ***set aside the resolution*** on the grounds that
* there is no reasonable basis for believing the company is financially distressed
* there is no reasonable prospect of rescuing the company
* the procedural requirements for obtaining the resolutions were not complied with.

ii. ***set aside the appointment of the practitioner*** on the grounds that he or she
* is not qualified or
* is not independent of the company
* lacks the necessary skills.

3. SEC 131 – Court order to begin business rescue proceedings

3.1 An affected person may apply to the Court for an order to place the company under supervision and commence rescue proceedings.

3.2 An applicant (the affected person) must
* serve (send) a copy of the application on the company and the Commission and
* notify each affected person of the application.

NOTE (a): The court can place the company under supervision if it is satisfied that
i. the company is financially distressed
ii. the company has failed to pay over any amount in terms of an obligation in terms of a public regulation (e.g. pay municipal rates/levies), contract (e.g. pay creditor) or in respect of employment related matters, or
iii. it is just and equitable to do so for financial reasons and
iv. there is a reasonable prospect of rescuing the company.

CHAPTER 6 - Part B – Practitioner's functions and terms of appointment

1. SEC 140 – Powers and duties of practitioners

1.1 During the business rescue proceedings, the practitioner
i. has full management control of the company in substitution for its board and management
ii. may delegate any power to a person who was a member of the board or management
iii. may remove a member of management from office or appoint a person as part of management**.**

1.2 The practitioner is responsible for developing a business rescue plan and implementing it.

NOTE (a): During a company's business rescue proceedings the practitioner
* is an officer of the court and must report to the court as required
* has the responsibilities, duties and liabilities of a director of the company
* is not liable for any act or omission in good faith in the course of carrying out his function as practitioner, ***but*** can be held liable for gross negligence in respect of his performance as practitioner.

2. SEC 141 – Investigation of affairs of the company

2.1 As soon as practicable after being appointed, the practitioner must investigate the company's affairs, business, property and financial situation to evaluate whether there is a ***reasonable prospect of the company being rescued***.

2.2 If, at this stage, or at any stage of the business rescue proceedings, the practitioner concludes that there is ***no*** reasonable prospect of the company being rescued, the practitioner must
i. inform the court, the company and all affected persons of this fact and
ii. apply to the court for an order discontinuing the business rescue proceedings and placing the company in liquidation.

2.3 If at any time during the business rescue proceedings, the practitioner concludes that the company is ***not*** financially distressed, the practitioner must
i. inform the court, the company and all affected persons of this fact and apply to the court (where applicable) to set aside the business rescue proceedings or

ii. file a notice of termination of business rescue proceedings (with the Commission).

2.4 If at any time during the business rescue proceedings, the practitioner concludes that in the dealings of the company before business rescue proceedings began, there is evidence of

i. ***voidable transactions*** or
ii. ***a failure by the company or the directors to perform any material obligation***, the practitioner must take necessary steps to rectify the situation and may direct management to rectify the situation
iii. ***reckless trading, fraud or other contravention of any law*** relating to the company, the practitioner must forward the evidence to the appropriate authority (for further investigation and possible prosecution) and direct management to take the necessary steps to rectify the situation, including recovering any misappropriated assets of the company.

NOTE (a): When a company is financially distressed, shareholders and/or directors may be tempted to act in a manner which is reckless, fraudulent or which results in voidable transactions, e.g. a director purchasing one of the company's machines for an amount considerably below its market (fair) value, before the company is liquidated. In other words the shareholders/directors may place their own interests above those of the company and creditors, in an attempt to minimise their own losses.

3. SEC 142 – Directors to co-operate with and assist the practitioner

3.1 As soon as practical after business rescue proceedings begin, each director must deliver to the practitioner, all books and records that relate to the company which are in his possession, and if the director has knowledge of the whereabouts of other books and records, must inform the practitioner.

3.2 Within 5 business days after the business rescue proceedings begin, the directors must provide the practitioner with a statement of affairs of the company including as a minimum, particulars of

* any material transactions involving the company or its assets which occurred within the 12 months preceding the rescue proceedings
* any court, arbitration or administrative proceedings, the company is involved in
* the assets and liabilities of the company, and its income and disbursements within the preceding 12 months
* the number of employees and any agreements relating to the rights of employees
* debtors and creditors of the company, their rights and obligations.

CHAPTER 6 - Part C – Rights of affected persons during business rescue proceedings

1. SEC 144, 145, 146 –Rights of affected persons during business rescue proceedings

1.1 For the purposes of this text the detail of these sections is not important, but it is essential to understand that a business rescue plan is a collective effort by the practitioner ***and*** affected persons to save the company. The Act draws employees, creditors and holders of the company's securities into the process by stipulating the "rights" these groupings have.

In general terms employees, trade unions, creditors and holders of the company's securities, are entitled to

i. receive notice of each court proceedings, decision, meeting or event relating to the business rescue plan
ii. participate in court proceedings
iii. form representative committees
iv. be consulted by the business rescue practitioner
v. be present and make submissions at meetings of the holders of voting interests

vi. vote on the approval of the business rescue plan
vii. propose and develop an alternative business plan if the (practitioner's) proposed rescue plan is rejected.

2. SEC 147 and 148 – First meetings of creditors and employees' representatives

2.1 In terms of these sections the practitioner must, within 10 days of being appointed, convene and preside over a first meeting of creditors and a (separate) first meeting of employees' representatives.

2.2 The purpose of these meetings is to inform these groups whether the practitioner believes that there is a reasonable prospect of rescuing the company.

NOTE (a): The practitioner must give notice of the respective meetings to every creditor, and employee (trade union if applicable) setting out the date, time and place of the meeting, and the agenda for the meeting.

CHAPTER 6 - Part D – Development and approval of business rescue plan

1. SEC 150 to 154 – Development and approval of business rescue plan

1.1 It is the duty of the practitioner, after consulting the creditors, management and other affected parties to prepare a business rescue plan.

1.2 The plan must contain all the information required to facilitate affected persons in deciding on whether to accept or reject the plan. The plan must de divided into three parts (this is a requirement of Sec 150)
* Part A - background
* Part B – proposals
* Part C – assumptions and conditions,

and must conclude with a certificate by the practitioner stating that
* actual information provided appears accurate, complete and up to date
* projections provided are estimates made in good faith on the basis of factual information and the assumptions set out in the plan.

1.3 The business plan must be published within 25 business days after the date on which the practitioner was appointed (this can be extended by the court or the majority of creditors' voting interests).

1.4 The practitioner must in terms of Sec 151, then convene and preside over a meeting of creditors and other holders of a voting interest to consider the plan. (This must occur within 10 business days of publishing the plan).

1.5 Approval on a preliminary basis will then be sought from the creditors, if more than 75% of the creditor voting interests support the plan, preliminary approval is obtained.

1.6 If the rescue plan does ***not*** alter the rights of the holders of any class of the company's securities, the preliminary approval becomes final approval and the plan is adopted.

1.7 If the rescue plan does alter the rights of the holders of any class of such securities, the practitioner must convene a meeting of those security holders and put the plan to the vote. If a majority (over 50%) of the affected security holders vote to adopt the plan, the preliminary approval becomes final approval and the plan is adopted.

1.8 If the rescue plan is rejected, the practitioner may seek approval to prepare and publish a revised plan. If this is granted the "prepare, publish, approve procedure" will be carried out again.

NOTE (a): If the practitioner or an affected person, believes that the decision to reject the rescue plan was egregious (outstandingly bad), irrational or inappropriate, he may apply to the court to set aside the result of the vote.

CHAPTER 6 – Part E – Compromise with creditors

1. SEC 155 – Compromise between company and creditors

1.1 The board of a company or the liquidator of such company if it is being wound up, may propose an arrangement or compromise of its financial obligations to its creditors.

1.2 Any such proposal must be divided into three parts namely
* Part A – Background
* Part B - proposals
* Part C – Assumptions and Conditions and

must include a certificate by an authorized director stating that:
* factual information provided appears to be accurate, complete and up to date
* projections provided are estimates made in good faith on the basis of the factual information and assumptions in the proposal.

NOTE (a): Such a proposal will be binding on all affected creditors if the proposal is supported by a ***majority in number of creditors*** who represent at ***least 75% in value*** of the creditors.

CHAPTER 7 – REMEDIES AND ENFORCEMENT

The detail of this chapter is expected to be outside the requirements of SAICA and the IRBA, but it is important for students to have a broad understanding of what is contained in the chapter. Much of what is contained in the chapter is unlikely to affect the everyday practice of auditing, and will be more relevant to lawyers. Thus only a few sections have been included in these summaries along with brief comment where appropriate.

CHAPTER 7 - Part A – General principles

1. SEC 156 – Alternative procedures for addressing complaints or securing rights

1.1 The essence of this section is to provide a range of persons (in various forms) with ways of proceeding against a company and/or its directors to
* address alleged contraventions of the Act or
* enforce any provision, or right in terms of the Act, of the company's Memorandum of Incorporation or rules and

to provide mechanisms for addressing complaints or securing rights.

NOTE (a): In terms of this section, a person may attempt to resolve a dispute by
i. mediation, conciliation or arbitration with the company
ii. applying to the Companies Tribunal for adjudication
iii. applying to the High Court
iv. applying to the Companies and Intellectual Property Commission
v. applying to the Takeover Regulation Panel.

The route the complainant takes depends on the nature of the dispute.

2. SEC 158 –Remedies to promote purpose of the Act

2.1 When deliberating on any matter, the court must develop the common law to improve the realization and enjoyment of rights established by the Act, and all parties to whom disputes are referred (including the court) must promote the spirit, purpose and objects of the Act.

3. SEC 159 –Protection for whistle blowers

3.1 The purpose of this section is to provide protection e.g. against dismissal, demotion, court action etc, for a shareholder, director, secretary, prescribed officer or employee of a company, representative of employees (e.g. trade union), a supplier of goods or services to the company or an employee of such a supplier, who discloses information about the company or the directors (whistle blowing).

NOTE (a): The section covers disclosures made in ***good faith*** to the Commission, the Companies Tribunal, the Takeover Regulation Panel, a regulatory authority, an exchange, a legal adviser, a director, prescribed officer, company secretary, ***auditor*** (internal or external)**,** board or committee of the company.

NOTE (b): The section covers information which showed or tended to show that the company or a director (or prescribed officer) has

i. contravened the Companies Act or any other Act enforced by the Commission e.g. Close Corporations Act, Copyright Act, Trade Marks Act as listed in Schedule 4, e.g. company selling counterfeit goods
ii. failed or is failing to comply with any legal obligation to which the company is subject e.g. company not paying VAT on cash sales
iii. engaged in conduct that has endangered or is likely to endanger the health or safety of any individual, or damage the environment e.g. company dumping toxic waste in a river
iv. unfairly discriminated, or condoned unfair discrimination, against any person as per Section 9 of the Constitution, e.g. company dismissing women who become pregnant
v. contravened any other legislation in a manner that could expose the company to an actual or contingent risk or liability, or is inherently prejudicial to the interests of the company, e.g. transport company bribing government officials to provide roadworthy certificates for its trucks without testing.

NOTE (c): In terms of this section, the whistle blower

i. has qualified privilege in respect of the disclosure and
ii. is immune from any civil, criminal or administrative liability for that disclosure.

NOTE (d): The company cannot override this section in its Memorandum of Incorporation or rules, e.g. it cannot include a clause which provides for instant dismissal of whistle blowers.

CHAPTER 7 - Part B – Rights to seek specific remedies

1. SEC 161 – Application to protect rights of securities holders

1.1 A holder of issued securities may apply to the court for an order to protect the rights pertaining to his securities (shares) in terms of the Act or the MOI or to rectify harm done to the securities by a company or any of the directors.

2. SEC 162 – Application to declare director delinquent or under probation

2.1 This section gives certain parties e.g. the company, shareholders, director, company secretary, trade union, the power to apply to the court to have a director declared delinquent or under probation.

The section relates to a present director or an individual who was a director within the 24 months preceding the application to the court.

3. SEC 163 – Relief from oppressive or prejudicial conduct

3.1 This section gives a shareholder or director the power to apply to the court for relief if
i. any act or omission of the company or
ii. the manner in which the business of the company has been conducted or
iii. the abuse of his powers by a director etc,
has had a result which is oppressive or unfairly prejudicial to, or unfairly disregards, the interests of the applicant.

NOTE (a): If the court finds in favour of the applicant, it may make any interim or final order it considers fit. These range from an order restraining the conduct complained of, to appointing additional directors, to ordering compensation to an aggrieved party.

CHAPTER 7 - Parts C to F - The remaining sections in this chapter of the Companies Act 2008 are mainly procedural and are beyond the scope of this text.

CHAPTER 8 – REGULATORY AGENCIES AND ADMINISTRATION OF ACT

This chapter establishes four "regulatory agencies", lays out their objectives and functions, gives them powers and determines how they should be staffed. It is not necessary to detail all of the above, however, prospective auditors should be aware of the agencies and their broad functions, particularly the Financial Reporting Standards Council. A brief overview of the agencies is given below.

CHAPTER 8 - Part A – Companies and Intellectual Property Commission

1. SEC 185 to 192 – Establishment, Objectives, Functions, etc

1.1 The Commission is a juristic person which must be independent and must perform its functions impartially, without fear, favour or prejudice.

1.2 Its objectives are to
* efficiently and effectively register companies, other juristic persons arising from various Acts under its control (see Schedule 4) and intellectual property rights.
* maintain up to date, accurate and relevant information pertaining to companies etc
* promote awareness of company and intellectual property laws
* promote compliance with the Act and other applicable legislation
* enforce the Companies Act and other Schedule 4 Acts.

1.3 The Commission is also responsible for advising the Minister on national policy relating to companies and intellectual property law.

1.4 The Commission will be headed by a Commissioner and Deputy Commissioner, both appointed by the Minister. Specialist Committees may be appointed by the Minister to advise on matters relating to company law or policy as well as on the management of the Commissions resources.

CHAPTER 8 - Part B – Companies Tribunal

1. SEC 193 to 195 – Companies Tribunal

1.1 The Companies Tribunal is a juristic person which must be independent and must perform its functions impartially and without fear, favour or prejudice, and in an appropriate transparent manner.

1.2 The Minister will appoint the chairperson and other members (at least 10) of the Tribunal. Members must comprise persons suitably qualified and experienced in economics, law,

commerce, industry or public affairs. The Minister must designate a member of the tribunal as deputy chairperson.

1.3 The functions of the Companies Tribunal are to
* adjudicate in relation to any application made to it in terms of the Act
* assist in voluntary resolutions of disputes
* perform any function allocated to it in terms of the Companies Act or any Act mentioned in schedule 4.

CHAPTER 8 - Part C – Takeover Regulation Panel

1. SEC 196 to 202 – Establishment, composition, functions, etc

1.1 The Takeover Regulation Panel is a juristic person which must be independent and must perform its functions impartially without fear, favour or prejudice.

1.2 The Panel will be made up of the Commissioner, various other stipulated persons (posts) and a number of other individuals appointed by the Minister. The Minister may designate members of the Panel to be chairperson and deputy chairpersons (two). The panel may appoint an executive director and one or more deputy executive directors.

1.3 The functions of the Panel are to
i. regulate affected transactions, and investigate complaints relating to affected transactions (amalgamations, mergers etc)
ii. apply to the court to wind up a company where the directors etc have acted fraudulently or illegally and have not responded to compliance "warnings" by the Commission or Panel itself
iii. consult the Minister in respect of changes to the Takeover Regulations.

1.4 Sec 202 provides for the establishment of a Takeover Special Committee to hear and decide on any matter referred to it by the Panel or, if applicable, the Executive Director of the Panel.

CHAPTER 8 - Part D – Financial Reporting Standards Council

1. SEC 203 and 204 – Establishment, composition and functions

1.1 The functions of the Council are to
i. receive and consider any relevant information relating to the reliability of, and compliance with financial reporting standards and adopt international reporting standards for local circumstances
ii. advise the Minister on matters relating to financial reporting standards and
iii. consult with the Minister on the making of regulations establishing financial reporting standards.

1.2 The Minister is responsible for establishing a committee (called the Financial Reporting Standards Council) by appointing suitably qualified persons, in terms of the requirements of the Act, e.g. four practicing auditors, two persons responsible for preparing financial statements for a public company, two people knowledgeable on company law, a person nominated by the Governor of the South African Reserve bank, etc (See Sec 203).

CHAPTER 8 - Part E – Administrative provisions applicable to agencies

The balance of the sections in this chapter of the Companies Act 2008 are generally procedural and are beyond the scope of this text.

CHAPTER 9 – OFFENCES, MISCELLANEOUS MATTERS AND GENERAL PROVISIONS

CHAPTER 9 - Part A – Offences and Penalties

1. SEC 213 – Breach of confidence

1.1 It is an offence to disclose any confidential information concerning the affairs of any person obtained in carrying out any function in terms of this Act or participating in any proceedings in terms of the Act.

NOTE (a): Obviously this does not apply to information disclosed
* for the purpose of proper administration or enforcement of this Act
* for the purpose of administering justice
* at the request of a regulatory agency (or its inspectors) entitled to receive the information or
* when required to do so by any court or under any law.

NOTE (b): In terms of Sec 216, a person convicted of breaching this section is liable to a fine or imprisonment not exceeding 10 years, or to both!

2. SEC 214 – False statements, reckless conduct and non-compliance

2.1 A person is guilty of an offence if he
* is party to the falsification of any accounting records
* knowingly provided false or misleading information, with a fraudulent purpose, in any circumstance in which the Act requires the person to provide information.
* was knowingly a party to an act or omission calculated to defraud a creditor, employee or security holder or with another fraudulent purpose.
* is a party to the preparation, approval, dissemination or publication of
  - financial statements, knowing that the financial statements do not comply with the requirements of Sec 29(1) e.g. do not satisfy the financial reporting standards, do not indicate whether they have been audited or not. (See Section 29 (6)).
  - financial statements, knowing that they are false or misleading
  - a prospectus which contains an untrue statement.

NOTE (a): Again in terms of Sec 216, a person convicted of breaching this section is liable to a fine or imprisonment not exceeding 10 years, or to both.

3. SEC 215 – Hindering administration of the Act

3.1 It is an offence to hinder, obstruct or improperly attempt to influence the Commission, the Companies Tribunal, the Panel , an investigator/inspector or the court when any of them is exercising a power or duty in terms of the Act.

NOTE (a): A breach of this section may result in a fine or imprisonment not exceeding 12 months, or both.

CHAPTER 9 - Part B – Miscellaneous matters – nil

CHAPTER 9 - Part C – Regulations etc

1. SEC 225 – Short title

1.1 This Act will be called the Companies Act, 2008.

THE CLOSE CORPORATION ACT 1984

1. INTRODUCTION

The idea of a close corporation is that the members all work together for the good of the whole and in doing so, they monitor each others actions, thus making strict external regulation less important.

The Close Corporations Act No. 69 of 1984 created a legal entity which was far simpler than a company to administer and which required far less formality. With the introduction of the Companies Act 2008, the formation and administration of companies has been simplified to the extent that the option of a close corporation as a business entity has been withdrawn effective from the date on which the Companies Act 2008 came into operation, i.e. 1 May 2011. Existing close corporations can convert themselves into companies or may elect to remain as close corporations. Those CCs which do not convert will, for the time being, be controlled by the existing Close Corporations Act 1984 but there have been some ***important amendments*** to this Act to bring it into line with the Companies Act 2008.

At its inception, the Close Corporations Act was built around what has been termed the liquidity/solvency principle, as opposed to the capital maintenance concept, around which the former Companies Act was built. The Companies Act 2008 moves away from the capital maintenance concept, towards the liquidity/solvency principle. Simplistically, the capital maintenance concept requires prohibitions or strict requirements to be in place in respect of transactions involving the capital of a company. This is in contrast to the liquidity/solvency principle which primarily requires that the liquidity and solvency of the entity remain intact after any transaction relating to the capital of the entity.

2. IMPORTANT CHANGES TO THE CLOSE CORPORATIONS ACT 1984

2.1 Now that the Companies Act 2008 is effective, no new close corporations can be formed. An existing close corporation can be converted to a company or continue to operate as a close corporation in terms of the Close Corporations Act 1984.

2.2 Requirements for the transparency and accountability of close corporations have been enhanced. Most significant of these changes is that Section 10 of the Close Corporations Act has been amended to include the requirement that "Regulations made by the Minister in terms of the Companies Act 2008, sections 29(4) and (5) and 30(7) will apply to a close corporation". In effect this means that:

* every CC must calculate its public interest score
* prepare its financial statements in terms of the financial reporting standards relevant to its public interest score
* some CCs will need to be audited depending on their public interest scores and whether their financial statements are internally or independently compiled.

2.3 Chapter 6 of the Companies Act 2008 which deals with the rescue of financially distressed companies will apply to Close Corporations as well.

3. CALCULATION OF THE CLOSE CORPORATIONS PUBLIC INTEREST SCORE

3.1 The score must be calculated annually as follows. It will be the sum of the following:

(i) a number of points equal to the average number of employees of the CC during the financial year
(ii) one point for every R1m (or portion thereof) in third party liabilities of the CC at the financial year end
(iii) one point for every R1m (or portion thereof) in turnover of the CC during the financial year and
(iv) one point for every individual who, at the end of the financial year, is known by the CC to directly or indirectly have a beneficial interest in the CC.

4. PREPARATION OF FINANCIAL STATEMENTS

4.1 As indicated above, the public interest score will determine which financial reporting standards will apply to the close corporation.

4.2 The options are essentially IFRS, IFRS for SMEs.

5. AUDIT REQUIREMENT

5.1 The public interest score and activity of the CC as well as whether the financial statements were internally or independently compiled, will determine the audit requirement.

5.2 The following CCs must be audited

* any CC in the ordinary course of its primary activities, holds assets (which had an aggregate value of R5m at any time during the year) in a fiduciary capacity for persons who are not related to the close corporation.
* any CC with a public interest score of 350 or more or
* any CC with a public interest score of at least 100 but less that 350, if its financial statements were internally compiled.

6. BREAKDOWN OF THE CLOSE CORPORATIONS ACT BY PART

The Close Corporation Act itself is broken up into 10 parts each dealing with separate aspects. The following list identifies those sections which are regarded as important for a general understanding of the Act.

Definitions		:	Refer to when studying individual sections
Part I	Formation	:	Section 2
Part II	Administration of Act	:	Sections 5, 10
Part III	Registration etc	:	Sections 12, 17, 22, 23, (27 withdrawn)
Part IV	Membership	:	Sections 29, 33, 35, 36, 37, 39, 40
Part V	Internal Relations	:	Sections 42, 43, 44, 46, 47, 48, 49, 51, 52
Part VI	External Relations	:	Sections 53, 54
Part VII	Accounting and Disclosure	:	Sections 58, 59,62
Part VIII	Liability of Members	:	Sections 63, 64
Part IX	Winding up	:	Nil
Part X	Penalties	:	Nil

SECTION SUMMARIES AND NOTES

PART I FORMATION AND JURISTIC PERSONALITY

1. SEC 2 - Formation and juristic personality

1.1 New close corporations can no longer be formed with the introduction of the Companies Act 2008. However, close corporations which were in existence prior to 1 May 2011 (the date on which the Companies Act 2008 became effective) continue to exist.

1.2 The original requirement that the CC must have one or more members but not more than 10 still applies (Sec 28).

PART II ADMINISTRATION OF THE ACT

1. SEC 5 - Inspection of documents

1.1 Any person can, on payment of the prescribed fee and subject to the availability of the original document
* inspect any document kept by the Companies and Intellectual Property Commission in respect of a corporation or,
* obtain a certificate from the Companies and Intellectual Property Commission as to the contents of any such document
* obtain a copy or extract from any such document.

NOTE (a): The administration of the CC Act now falls under the Companies and Intellectual Property Commission.

2. SEC 10 - Regulations and policy

2.1 Regulations made by the Minister in terms of the Companies Act 2008, Sec 29(4) and (5) relating to the preparation of financial statements in terms of the financial reporting standards, and Sec 30(7) relating to audit requirements, will now apply to close corporations (see discussion in the introduction to close corporations).

PART III REGISTRATION, DEREGISTRATION AND CONVERSION

1. SEC 12 - Founding statement

1.1 The ***founding statement*** is the basic document which brought all existing CCs into being.

1.2 It is signed by all members who formed the CCs and contains:
* the name of the CC
* principal business of the CC
* postal address, physical address
* full name and ID of each member
* the percentage of each member's interest
* particulars of each member's contribution (Sec 24)
* the accounting officer's name and address
* the date of the financial year-end.

NOTE (a): This document equates partially to the ***memorandum of incorporation*** of a company.

NOTE (b) Founding Statements of existing CCs are lodged with the Commission (Sec 13).

NOTE (c) All existing CCs have a CC registration number, and are issued with a certificate of incorporation (Sec 14)).

NOTE (d): Any changes to the information in the founding statement will result in an ***amended founding statement*** having to be lodged (Sec 15). Circumstances at existing CCs can still result in the need for an amended founding statement e.g. a new member may join the CC.

NOTE (e) Each year the CC must lodge an ***annual return*** to confirm the validity of the CC's founding data (Sec 15A).

NOTE (f): A CC must keep a copy of its founding statement and annual return at its registered office.

2. SEC 17 - No constructive notice of particulars in founding statement

2.1 No person shall be deemed to have knowledge of any information in the founding statement simply by virtue of the fact that it is lodged with the Registrar.

3. SEC 22 - Formal requirements as to names.

3.1 A CC must attach the letters CC (or other official language abbreviation) to its name.

4. SEC 23 - Use and publication of names

4.1 Essentially Sec 23 of the CC Act states that the CC must comply with Sec 32 of the Companies Act

* A CC must provide its full registered name or registration number to any person on demand.

* A CC must not misstate its name or registration number in a manner likely to mislead or deceive any person.

* The name and number must also appear on all notices, publications and stationery, e.g. bills of exchange, cheques, invoices, etc (whether hardcopy or electronic).

NOTE (a): This requirement is to ensure that people dealing with the CC are aware that they are dealing with a "juristic person" in its own right.

5. SEC 27 - Conversion of companies into corporations.

NOTE: This section has been withdrawn and it is no longer possible for a company to convert to a CC. It is possible for a CC to convert to a company. The procedure is dealt with in Schedule 2 of the Companies Act 2008.

5.1 Schedule 2 Sec 1(1). A close corporation may file a notice of conversion in the prescribed manner and form ***at any time*** with the Commission.

5.2 A notice of conversion must be accompanied by

* a written statement of consent approving the conversion of the CC to a company (signed by members holding at least 75% of the members' interests)
* a Memorandum of Incorporation.
* a prescribed filing fee.

5.3 After acceptance of a notice of conversion, the Commission must

* assign to the (new) company, a unique registration number
* enter the details of the company in the companies register
* endorse the notice of conversion and MOI filed with it and
* issue a registration certificate to the (new) company
* cancel the registration of the close corporation
* give notice in the Gazette of the conversion and enable the Registrar of Deeds to effect necessary changes resulting from conversion and name changes.

NOTE (a): Every member of the CC is entitled to become a shareholder of the (new) company
* the shareholders in the company need not necessarily be in the same proportion as the members' interests were in the CC
* a member of the CC who does not wish to become a shareholder in the company does not have to become a member, and would arrange for the disposal of his interest prior to the conversion.

NOTE (b): On the registration of the (new) company
* the juristic person that existed as a CC continues to exist as a juristic person but in the form of a company
* all the assets, liabilities, rights and obligations of the CC vest in the (new) company
* any legal proceedings instituted against the CC may be continued against the (new) company
* any enforcement measures that could have been instituted against the CC can be brought against the (new) company
* any liability of a member of the CC arising out of the Close Corporation Act, continues as a liability of that person as if the conversion has not taken place.

For all practical purposes things remain the same.

PART IV MEMBERSHIP

1. SEC 29 - Requirements for membership

1.1 Subject to some exceptions, only ***natural persons*** may be members of a close corporation.

1.2 A natural person will qualify for membership
* if he is entitled to a members' interest (i.e. made a contribution or purchased the interest)
* in his ***official capacity*** as a trustee of a ***testamentary trust*** provided that no juristic person is a beneficiary of the trust
* in his ***official capacity*** as a trustee, administrator, executor of an insolvent, deceased or mentally disordered member's estate or his duly appointed/authorized legal representative
* in his ***official capacity*** as trustee of an ***inter vivos*** trust (with certain provisos) e.g. no juristic person shall directly or indirectly be a beneficiary of the trust.

1.3 Joint memberships (two or more persons holding a single member's interest) are not allowed. (Sec 30).

1.4 The intention of the legislature is to keep membership as ***natural*** as possible so that the "closeness" of the corporation is not complicated by juristic entities (non-people!).

1.5 A corporation may have one or more members, but not more than ten. (Sec 28).

2. SEC 33 - Acquisition of a member's interest

2.1 There are two ways to acquire a members' interest:
* Pursuant to a contribution made to the *CC:* other members' interests will be amended accordingly (total must always equal 100%)
* Purchase from an existing member/members: no contribution to the CC is made.

NOTE (a): A member's interest will be expressed as a percentage and will be regarded as moveable property (Sec 30).

NOTE (b): Each member will be issued with a membership certificate which states the interest percentage held by the member (Sec 31).

3. SEC 35 – Disposal of interest of deceased member

3.1 The executor of a deceased member's estate will arrange the transfer of the deceased

member's interest to an heir, if

* the heir is eligible (qualifies) for membership of a close corporation, and
* the remaining members consent thereto.

NOTE (a): If the other members' consent if not given within 28 days of it being requested, the executor may

* sell the interest to the corporation (if there is another member or other members)
* sell the interest to any other remaining member(s)
* sell the interest to any other person who qualifies for membership. In this case, the other members (if any) will have the right to reject the "other person" and purchase the interest themselves. They may not approve of the person to whom the executor intends to sell the interest.

NOTE (b): The association agreement may stipulate other arrangements in respect of the deceased member's interest. The executor should adhere to these stipulations.

4. SEC 36 - Cessation of membership by order of the court

4.1 On application of any member, the Court may rule that a member shall cease to be a member on any of the following grounds:

4.1.1 The member is permanently incapable of performing his role e.g. ***unsound mind***.

4.1.2 The member is guilty of conduct which is likely to be prejudicial to the business e.g. ***negligence or recklessness on the part of the member.***

4.1.3 The other members find it impractical to carry on business due to the conduct of the member e.g. ***such member is never present.***

4.1.4 Circumstances have arisen which render it just and equitable that such a member should cease to be a member e.g. ***the member continues to act in his own interests to the detriment of the CC.***

NOTE (a): This section is designed to protect members against members who do not "***pull their weight***" one way or another.

NOTE (b): The court, in ruling on this matter, may order as it deems fit with regard to the acquisition of the departing member's interest by the other members and the amount and method of payment therefore.

5. SEC 37 - Disposition of a member's interest (other than insolvent, deceased and Sec 36 dispositions).

5.1 A member may dispose of his interest to:

5.1.1 The corporation itself.

5.1.2 Any other person (qualified for membership) provided that the disposition is made in terms of the association agreement (if any) ***or*** with the consent of every other member of the corporation.

6. SEC 39 - Payment by the corporation itself where it acquires a member's interest

6.1 The CC itself may acquire a member's interest provided:

6.1.1 Every member other than the selling member has given ***prior written consent.***

6.1.2 After payment for the member's interest, the assets, fairly valued, exceed the CC's liabilities (solvency).

6.1.3 The corporation is able to pay its debts as they become due (liquidity).

6.1.4 The payment itself does ***not*** render the corporation unable to pay its debts as they become due.

7. SEC 40 - Financial assistance given by corporation in respect of acquisition of member's interests

7.1 A CC may give financial assistance directly or indirectly, in any form, for the purchase of a member's interest.

7.2 The requirements indicated in 6.1.1 to 6.1.4 must be adhered to.

PART V INTERNAL RELATIONS

1. SEC 42 - Fiduciary position of the members.

1.1 Each member of the CC stands in a fiduciary relationship to the corporation.

1.2 This means that the member must:

1.2.1 Act honestly and in good faith.

1.2.2 Exercise his powers to manage or represent the corporation in the interests of and for the benefit of the corporation.

1.2.3 Not act without, or exceed the power he has been granted.

1.2.4 Avoid conflict between his own interests and those of the corporation; in particular:

* not derive personal economic benefit in conflict with the corporation
* notify every other member at the earliest opportunity of the nature and extent of any personal "interest in contracts" of the corporation
* not compete in any way with the corporation in its business activities.

NOTE (a): Remember a CC is a separate legal entity, hence the fiduciary duty between itself and the members arises.

NOTE (b): A member who breaches his fiduciary duty shall be liable to the corporation for

* any loss suffered by the corporation as a result thereof
* any economic benefit derived by the member as a result thereof.

NOTE (c): A member will not be in breach of any fiduciary duty if his conduct was preceded or followed by the written approval of all members provided that all the members were cognizant (aware) of the facts.

NOTE (d): The detail of how and when a "member's interest in contracts" should be disclosed is not specified (the Act does not seek to regulate internal relations too strictly). However, ***logic*** should apply, but where a member fails to disclose his interest, the contract will be ***voidable*** at the option of the corporation.

2. SEC 43 - Liability for negligence

2.1 If a member fails to act with the care and skill that may reasonably be expected from a person of his knowledge and experience, he will be ***liable for any loss*** suffered by the corporation as a result of that failure.

NOTE (a): Negligence is a separate issue from breach of contract - a member could be guilty of both.

NOTE (b): Once again written approval of a member's "negligent" action by all of the members, if they are cognisant of the facts, will render this section ineffective.
Any member of the CC may proceed against a fellow member of the CC in relation to Sec 42 and Sec 43. Such member must notify the other members of his intention to do so.

3. SEC 44 - Association agreements

3.1 Association agreements are voluntary.

3.2 An existing association agreement is binding on all present and new members.

3.3 Its aim is to regulate the internal affairs of the corporation.

3.4 There is no constructive notice with regard to association agreements. (Sec 45).

3.5 The agreement may be altered or dissolved. Amendments and dissolutions must be in writing and signed by each member.

4. SEC 46 - Variable rules regarding internal relations

4.1 The following rules will apply ***unless they are replaced or varied by an association agreement***

- 4.1.1 Every member is entitled to participate in the carrying on of the business.
- 4.1.2 Every member has equal rights in respect of the ***management*** of the business.
- 4.1.3 For the following transactions, consent in writing of members (or a member) holding at least 75% of the members' interests will be required
  - * a change in the principal business,
  - * a disposal of the whole, or substantially the whole undertaking of the corporation,
  - * a disposal of all, or the greater portion of the assets,
  - * any acquisition or disposal of immovable property by the corporation.
- 4.1.4 Differences between members will be decided by a majority vote of members.
- 4.1.5 At any meeting, the members of the corporation shall have the number of votes which corresponds with his percentage interest.
- 4.1.6 A corporation shall indemnify every member in respect of expenditure incurred or to be incurred by him (on behalf of the corporation).
- 4.1.7 Payments as defined (see pt.8) shall be made in terms of agreement between members but in proportion to their members' interest.

5. SEC 47 - Disqualification from managing the business of the corporation

5.1 This section identifies persons who are disqualified from the management of a close corporation. The section has been aligned with the Companies Act 2008 particularly Sec 69(8) to (11) of the Act.

5.2 In terms of Sec 69(8) to (11) of the Companies Act 2008, a person is disqualified from taking part in the management of the corporation if:

- 5.2.1 A court has prohibited that person from being a director or has declared that person to be ***delinquent*** or on ***probation*** in terms of Sec 162 of the Companies Act. This section covers such situations as
  - * a person acting as a director when disqualified or ineligible to do so
  - * a director grossly abusing the position as a director
  - * a director taking personal advantage of information
  - * a director, intentionally or by gross negligence, inflicting harm on the company
  - * a director acting in a manner that amounted to gross negligence, wilful misconduct or breach of trust in relation to the performance of his duties.
- 5.2.2 The person is an unrehabilitated insolvent.
- 5.2.3 The person is prohibited in terms of any public regulations from being a director.
- 5.2.4 The person has been removed from an office of trust, on the grounds of misconduct involving dishonesty.
- 5.2.5 The person has been convicted in the Republic or elsewhere, and imprisoned without the option of a fine, or fined more than the prescribed amount (prescribed in the Regulations) for theft, fraud, forgery, perjury or an offence
  - * involving fraud, misrepresentation or dishonesty

* in connection with the promotion formation or management of a company etc, or
* under the Companies Act, Insolvency Act, CC Act, Competition Act, Financial Intelligence Centre Act, Securities Act or Chapter 2 of the Prevention and Combating of Corruption Activities Act.

NOTE (a): A court may exempt a person from a disqualification imposed in terms of 5.2 above.

NOTE (b): As a general rule disqualifications arising from 5.2.4 or 5.2.5 end 5 years after the date of removal from office or the completion of the sentence. However, the commissioner may apply for an extention of the disqualification period.

NOTE (c): This section disqualifies persons from ***managing*** the company. It does not ***prevent*** them from becoming members. Membership is determined in terms of Sec 29.

NOTE (d): Despite being disqualified by Sec 69 of the Companies Act, a member of a CC may participate in the management of the CC if 100% of members' interests are held by that person, or that person and other persons, all of whom are related to that disqualified person and have consented in writing to that person participating in management. e.g. a husband and wife may hold all the members' interests. The wife can consent to the husband continuing to manage the CC even if he is disqualified in terms of Sec 69.

6. SEC 48 – Meetings of members

6.1 Any member of a corporation may, by notice to every other member, call a meeting of members for any purpose disclosed in the notice.

6.2 Unless the association agreement provides otherwise (i.e. stipulates specific requirements for meetings)
* the notice of the meeting must stipulate "reasonable" date, time and venue
* three quarters of the members present, in person, shall constitute a quorum
* only members present, in person, may vote.

7. SEC 49 - Unfairly prejudicial conduct

7.1 A member who believes that any particular act or omission of the corporation or by one or more of the members is ***unfairly prejudicial, unjust or inequitable*** to him, or to some members including him, may make an appeal to the Court.

NOTE (a): In settling the dispute, the Court may make such order it deems fit including the purchase of the aggrieved member's interest by the corporation.

NOTE (b): This section is a form of protection for members against other members.

8. SEC 51 - Payments to members

8.1 A payment (as defined) to a member may only be made if the ***liquidity/solvency*** requirements are met.

NOTE (a): "Payments" in this section refer to payments made to a member specifically by virtue of the fact of that membership. This includes:
* repayment of a member's contribution
* a distribution of profits.

NOTE (b): If the payment is being made by virtue of any other contractual obligation e.g. the member is also a creditor, or earns a salary for services to the corporation, then it is not subject to the liquidity/solvency test.

NOTE (c): "Payments" do not need to be in cash to be subject to this section, for example, transfer of property would also qualify.

NOTE (d): This section protects creditors of the corporation from the members "bleeding" the corporation to the creditors' detriment.

NOTE (e): Members will be liable to the corporation for any payment received contrary to this section.

9. SEC 52 - Loans (security) to members and others

9.1 A close corporation shall not make a loan ***directly or indirectly:***
- 9.1.1 To any of its members.
- 9.1.2 Any other corporation in which one or more of its members together hold more than 50%.
- 9.1.3 Any company or other juristic person controlled by one or more member of the corporation.

9.2 This section shall not apply where the (***previously obtained) consent of all members in writing is obtained***.

NOTE: Any member who authorises or permits a loan contrary to the requirements of this section, will be liable to indemnify the corporation against any loss resulting from the invalidity of such loan.

PART VI EXTERNAL RELATIONS

1. SEC 53 – Pre- incorporation contracts

1.1 Any contract entered into by a person professing to act as an agent or a trustee for a corporation yet to be formed, will be deemed to have been entered into as if the corporation had been formed if:
- 1.1.1 The contract is in writing
- 1.1.2 It is, after incorporation, ratified or adopted
- 1.1.3 By all members, in writing
- 1.1.4 Within the time stipulated by the contract or within a reasonable time.

NOTE (a): This section is included in the Act, but in reality should not be required because ***since 2011 no new close corporation could or can be formed.***

2. SEC 54 - Power of members to bind the corporation

2.1 Any act of a member will bind the corporation if:
- 2.1.1 Such act is expressly or impliedly authorised by the corporation ***or***
- 2.1.2 If the act is performed in the usual way of the corporation's business (as stated in the founding statement) or in terms of the business actually being carried on by the corporation at the time of the act ***unless***
  - * the said member had no power to act ***and***
  - * the 3rd party ought reasonably to have known that the member had no such power.

NOTE (a): The important distinction which needs to be made is whether the act falls within the scope of the CC's usual business.

If it does: The company ***will be bound*** regardless of whether the member had power to act, ***unless*** the CC can show that the 3rd party should have known that the member did not have power.

If it does not: The company ***will not be bound*** unless the 3rd party can prove that the member had authority, express or implied.

PART VII ACCOUNTING AND DISCLOSURE

1. SEC 58 - Annual financial statements

1.1 AFS must be made out within ***6 months*** of the year end in one of the official languages and must be approved by members' interests of at least 51%.

1.2 As discussed in the introduction to the notes on close corporations, every CC must calculate its public interest score and this will form the basis on which the close corporation must prepare its financial statements. A second consideration will be whether the CCs financial statements have been internally or independently prepared. The following diagram summarises these requirements.

Public Interest Score	Financial Reporting Standard	Audit Required?
Equal to or greater than 350	IFRS or IFRS for SMEs	Yes
At least 100 but less than 350 and AFS were ***internally*** compiled	IFRS or IFRS for SMEs	Yes
At least 100 but less than 350 and AFS were ***independently*** compiled	IFRS or IFRS for SMEs	No
Less than 100 and independently compiled	IFRS or IFRS for SMEs	No
Less than 100 and internally compiled	The financial reporting standard as determined by the company for as long as no financial reporting standard is prescribed	No

* Wherever IFRS for SMEs is an option, the CC must meet the scoping requirements outlined in the IFRS for SMEs.

* It appears that the Accounting Officers Report will be required to accompany all annual financial statements regardless of the financial reporting standard used or whether an audit was conducted.

2. SEC 59 - Appointment of accounting officers

2.1 Every close corporation must appoint an accounting officer

* accounting officer must be a member of a recognised (relevant) professional body which has been named in the Gazette e.g. SAICA, ACCA, CIMA, SAIPA, CIS (Sec 60).

2.2 If the members wish to remove the accounting officer, he must be notified by the members in writing
* if the accounting officer believes that he has been removed for improper reasons, he must notify the Registrar and every member in writing.

2.3 A member or employee of the close corporation, and a firm whose partner or employee is a member or employee of the corporation may be appointed accounting officer ***but*** all members must consent in writing (Sec 60).

2.4 The accounting officer may be a person, a firm of auditors (AP Act), any other firm or CC, provided each partner or member is qualified to be appointed.

3. SEC 62 - Duties of the accounting officer

3.1 Sec 61 provides the accounting officer with the right of access to the information needed to fulfil his duties.

3.2 The accounting officer (which a CC must have, and who must be a member of an accredited body) must:

Procedures
3.2.1 Determine whether the AFS are in agreement with the accounting records.
3.2.2 Review the appropriateness of the accounting policies used.

Report
3.2.3 Make a report in respect of the above.
3.2.4 Describe in his report any contraventions of the Act.
3.2.5 If applicable, state that he is a member or employee of the CC.

Commission
3.2.6 report to the Commission if:
* the CC is no longer carrying on business
* any changes to information required by the founding statement have not been reported
* at the year end the liabilities of the CC exceed its assets
* the financial statements ***incorrectly*** indicate that the assets of the corporation exceed its liabilities.

NOTE (a)**:** In terms of the Regulations, certain CCs will have to be audited. This will result in an audit report which will carry considerably more weight than an accounting officer's report. However, there is nothing in the legislation which says the accounting officer's report can be omitted where the CC is audited.

PART VIII LIABILITY OF MEMBERS AND OTHERS FOR THE DEBTS OF THE CC

1. SEC 63 - Joint liability for the debts of the corporation

This section must be read bearing in mind that it is designed to secure compliance with various provisions of the Act by exposing members to joint and several liability with the corporation for the debts of the corporation if they do not comply.

1.1 ***Abbreviation CC***
If the name of the corporation is used in any way without the abbreviation CC or equvalent, any member who is responsible for, or who authorized or knowingly permits the omission of the abbreviation, will be jointly and severally liable to any person who enters into any transaction with the corporation from which a debt accrues for the corporation while that person, as a result of the omission of the CC or equivalent abbreviation is unaware that he is dealing with a corporation.

1.2 ***Contribution payment outstanding***

Where a member fails to pay over his contribution to the CC, he will be liable for every debt of the corporation incurred from date of registration of the founding statement, to the date when the contribution payment is actually made by the member.

1.3 ***Invalid member***

Any juristic person or trustee of an inter vivos trust who purports to hold, directly or indirectly, a member's interest in contravention of Sec 29 – Requirements for membership, shall be liable for every debt of the corporation incurred during the time the contravention continued (despite the invalid membership).

1.4 ***Acquisition of members' interest***

Any payment made by a CC in respect of the acquisition of a members interest which does not have the prior written consent of all members, or does not meet the solvency/liquidity requirements, will result in every member (unless the member was unaware of the payment, or was aware but took all reasonable steps to prevent the payment), including the member who received the payment, being liable for the debts of the corporation incurred prior to making such payment.

1.5 ***Financial assistance***

Where the CC gives financial assistance for the acquisition of a member's interest in contravention of the Act, 1.4 shall apply.

1.6 ***Disqualified from management***

Where any person who is disqualified from ***managing*** the company, performs a management function, that person shall be liable for every debt of the corporation which it incurs as a result of that member's participation in management.

1.7 ***Vacancy : accounting officer***

Where the position of accounting officer has been vacant for a period of six months, any person who was a member of the corporation during the period and at the end of it, and was aware of the vacancy, is liable for every debt incurred by the corporation incurred during the six month period. The member will also be liable for debts incurred after the six month period until the vacancy is filled.

2. SEC 64 - Liability for reckless or fraudulent carrying on of business

2.1 The Court may, on the application of:

* the Master
* any creditor, member or liquidator of the company

declare that any person who was knowingly a party to the carrying on of the business ***recklessly, with gross negligence*** or with ***intent to defraud***, shall be ***personally*** liable for all or any debts or liabilities as the Court deems fit.

2.2 If any business of a close corporation is carried on in the manner described in 2.1, every person who is knowingly a party to the carrying on of the business in such manner, will be guilty of an offence.

PART IX WINDING UP - nil
PART X PENALTIES AND GENERAL – nil

THE AUDITING PROFESSION ACT 2005 (Act 26 of 2005)

1. INTRODUCTION

This Act plays an important role in the lives of all registered auditors and trainee accountants. It is the Act which created the Independent Regulatory Board for Auditors which has the responsibility of controlling the auditing profession in South Africa.

The preamble to the Act states that the Act is designed to :

* provide for the establishment of the Independent Regulatory Board for Auditors
* provide for the education, training and professional development of registered auditors
* provide for the accreditation of professional bodies
* provide for the registration of auditors and to
* regulate the conduct of registered auditors.

2. STRUCTURE OF THE ACT

The Act consists of 60 sections which are broken down into Seven Chapters. Many of the sections are not important for academic study purposes

Chapter 1	:	Interpretation and Objects of the Act
Chapter II	:	Independent Regulatory Board for Auditors
Chapter III	:	Accreditation and Registration
Chapter IV	:	Conduct by and Liability of Registered Auditors
Chapter V	:	Accountability of Registered Auditors
Chapter VI	:	Offences
Chapter VII	:	General Matters

SUMMARIES AND NOTES

CHAPTER I: INTREPRETATION AND OBJECTS OF THE ACT (sections 1 and 2)

In essence, this chapter provides definitions of words used in the Act and states that the objects of the Act are to

* protect the public by regulating audits performed by registered auditors
* provide for the establishment of an Independent Regulatory Board for Auditors
* improve the development and maintenance of internationally comparable ethical standards and auditing standards for auditors
* set out measures to advance the implementation of appropriate standards of competence and good ethics in the auditing profession and to
* provide for procedures for disciplinary action in respect of improper conduct.

CHAPTER II: INDEPENDENT REGULATORY BOARD FOR AUDITORS (sections 3 to 31).

This chapter is broken down into seven parts.

* ***Part 1*** establishes the IRBA as a ***juristic person*** and orders that the IRBA must exercise its functions in accordance with the Auditing Profession Act and any other relevant law. It also states that the IRBA is subject to the Constitution.

* ***Part 2*** spells out the functions of the IRBA. The matters which are dealt with include accreditation and registration, education, fees for being a member of IRBA, etc, promoting the integrity of the profession, prescribe standards, etc.

* ***Part 3*** gives the IRBA its general powers and its powers to make rules. General powers make it possible for the IRBA to operate, for example by giving it the power to appoint staff, enter agreements, acquire property, borrow money, etc. The power to make rules, allows the IRBA to execute its responsibilities in terms of the act.

* ***Part 4*** lays out the governance requirements of the Regulatory Board. These sections cover such matters as appointment of members of the Regulatory Board, their terms of office, disqualification from membership, meetings, the role of the Chief Executive Officer, etc, e.g. the Board must consist of not less than six but not more than 10 non-executive members appointed by the Minister.

* ***Part 5*** deals with committees of the Regulatory Board. Most significantly it lays down the requirement that at least the following permanent committees must be established :

Section 20 and 21	:	committee for auditor ethics
Section 20 and 22	:	committee for auditing standards
Section 20	:	an education, training and professional development committee
Section 20	:	an inspection committee
Section 20 and 24	:	an investigating committee
Section 20 and 24	:	a disciplinary committee

* ***Part 6*** deals with the funding and financial management of the Regulatory Board and covers the collection of fees, an annual budget and strategic plan, and the preparation of financial statements.

* ***Part 7*** deals with national government oversight and executive authority. This explains that the Minister of Finance is the executive authority for the IRBA, and that the IRBA is accountable to the Minister.

CHAPTER III: ACCREDITATION AND REGISTRATION (Sections 32 to 40).
This chapter is broken down into two parts.

* ***Part 1*** deals with the accreditation of professional bodies. For an individual to register with the IRBA, he must satisfy the prescribed education, training, competency and professional development requirements. As IRBA is not in the business of supplying the above, its model is to "outsource" these activities to professional bodies which it accredits. If an individual then satisfies the requirements of the accredited professional body, he or she may apply for registration with the IRBA. The only accredited professional body at the present time is SAICA.

* ***Part 2*** deals with the registration of individuals and firms as registered auditors and contains the following important sections :

1. SEC 37 – Registration of individuals as registered auditors

1.1 This section states that an individual may be registered if he
  * has complied with the prescribed education, training and competency requirements
  * is resident in the Republic
  * is a fit and proper person to practice the profession.

NOTE (a): If the individual is not a member of an accredited professional body, he will have to satisfy the IRBA that arrangements for his continuing professional development, have been made. (Note, an individual does not have to join SAICA to be registered with the IRBA.)

NOTE (b): On payment of the prescribed fee, the individual must be entered in the register and must be issued with a certificate of registration.

NOTE (c): The Regulatory Board may ***not*** register an individual who

* has at any time been removed from an office of trust because of misconduct related to carrying out duties relating to that office
* has been convicted and sentenced to imprisonment without the option of a fine, or to a fine exceeding a prescribed limit in the Republic or elsewhere, for fraud, theft, forgery, uttering (putting into circulation) a forged document, perjury or an offence under the Prevention and Combating of Corrupt Activities Act 2004
* is for the time being, of unsound mind or unable to manage his own affairs
* is disqualified from registration under a sanction imposed by the Auditing Profession Act, e.g. for a disciplinary matter.

NOTE (d): The Regulatory Board ***may decline*** to register an individual who

* is an unrehabilitated insolvent
* has entered into a compromise with creditors, or
* has been provisionally sequestrated.

2. SEC 38 –Registration of firms as registered auditors

The ***only*** firms that may be registered are

2.1 Partnerships of which all the partners are individuals who are themselves registered auditors.

2.2 Sole proprietors where the proprietor is a registered auditor.

2.3 Companies which comply with the following:

i The company must be incorporated and registered in terms of the Companies Act
* with a share capital and
* its Memorandum of Incorporation must provide that its directors and past directors shall be ***jointly and severally*** liable with the company for its debts and liabilities contracted during their periods of office.

ii Only individuals who are registered auditors may be shareholders. (If the company is to be a private company, its membership is ***not*** limited to 50).

iii Every ***shareholder*** must be a ***director*** and every ***director*** must be a ***shareholder.***

iv The Memorandum of Incorporation of the company provides that the company may, without the confirmation of the Court, purchase any shares held in it and allot those shares in accordance with the company's Memorandum of Incorporation.

v Only a shareholder may act as proxy for another shareholder, i.e. no outsiders may attend, speak or vote at, any meeting of the company. This must be stipulated in the MOI.

NOTE (a): An accounting company is required to comply with all sections of the Companies Act, e.g. produce annual financial statements, hold meetings, etc.

NOTE (b): Sec 38 ensures that registration with the IRBA is restricted to auditors, regardless of the form the firm takes. Registration requirements are strict. For example, an auditor and a lawyer cannot form a partnership and apply to be a firm of registered auditors. Likewise, a firm that wishes to constitute itself as a company, cannot include lawyers or others as shareholders or directors. Many auditing firms (partnerships and companies) have lawyers, engineers, IT specialists, on their staff but they cannot be partners or shareholders.

CHAPTER IV: CONDUCT BY AND LIABILITY OF REGISTERED AUDITORS (Sections 41 to 46).

1. SEC 41 – Practice

1.1 Only a registered auditor may engage in public practice.

1.2 A person who is not registered in terms of the AP Act, may not
* perform any audit (see notes (a), (c) and (e))
* pretend to be, or hold out to be, registered in terms of the AP Act (note (b))
* use the name of any registered auditor (see note (d))
* perform any act to lead persons to believe that he is registered in terms of The AP Act.

Remember: the term "audit" is defined as meaning an examination of, in accordance with applicable auditing standards:
i financial statements, with the objective of expressing an opinion as to their fairness in terms of an identified reporting framework or
ii financial and other information, prepared in accordance with suitable criteria with the objective of expressing an opinion on the financial and other information.

NOTE (a): This section does not prohibit a non-registered individual from performing an audit under the direction, control and supervision of a registered auditor, e.g. an employee in an auditing firm.

NOTE (b): An individual or firm may not use the descriptions "registered auditor", "public accountant", "registered accountant and auditor", "accountant in public practice", or any other designation likely to create the impression of being a registered auditor in public practice ***unless*** they are registered with the IRBA. Remember this is a prohibition created by law; it is similar to the medical profession, you cannot call yourself a medical doctor if you are not registered as such with the Health Professions Council of South Africa.

NOTE (c): The section does ***not*** prohibit
* any person from using the description "internal auditor" or accountant. Any person can offer accounting services (not auditing) to the public and call themselves a "financial advisor" or a "management accountant", etc
* any member of a not-for-profit club or similar entity, from acting as auditor for that club or entity, provided he receives no fee or other considerations for the audit
* the Auditor-General from appointing any person who is not a registered auditor, to carry out on his behalf, any audit in terms of the Public Audit Act 2004.

NOTE (d): For example, Joe Janks is a registered auditor practicing under the name of "J Janks Registered Auditor and Accountant". He retires and sells his practice to Paul Paris who is a very competent accountant but not eligible to register with the IRBA. Paul Paris would not be allowed to retain the name of the firm as "J Janks Registered Auditor and Accountant" and would not be able to retain the firms' audit clients.

NOTE (e): Except with the consent of the IRBA, a registered auditor may not knowingly employ
* any person suspended from public practice
* any person (formerly registered but) no longer registered as a result of the termination or cancellation of registration, or
* any person who was declined registration on the grounds of having been removed from an office of trust, convicted and sentenced for fraud, theft etc as laid out in Section 37, note (c).

NOTE (f): ***Section 41 (6)*** states that a registered auditor may ***not***

* practice under a firm name unless every letterhead bears the firm name, the first name (or initials) and surname of the registered auditor, the names of the managing or active partners in the case of a partnership, or in the case of a company, the names of the directors
* sign any account, statement, report or other document which purports to represent an audit unless the audit was performed by, or under the supervision of that auditor (or a co-partner or co-director) in accordance with prescribed auditing standards (see note (a))
* perform audits unless adequate risk management practices and procedures are in place
* engage in public practice if suspended
* share any profit derived from performing an audit with a person that is not a registered auditor.

NOTE (g): A registered auditor may sign the firm name, e.g. "PriceWaterhouse".

NOTE (h): A registered auditor must pay all prescribed fees to engage in public practice and in terms of Section 42, comply with all rules prescribed by the Regulatory Board.

2. SEC 44 – Duties in relation to an audit

2.1 In terms of Section 44 (1), where a firm accepts the appointment to perform an audit, it must immediately take a decision as to which ***individual*** registered auditor within the firm, will be responsible and accountable for the audit (see note (a)).

2.2 In terms of Section 44 (2) and (3) the registered auditor ***may not*** express an opinion, without qualification, that the financial statements

* fairly present in all material respects, the financial position of the entity and the results of its operations and cash flow, and
* are properly prepared in all material respects in accordance with the basis of accounting and financial reporting framework as disclosed in the financial statements

unless

* the audit has been carried out free of restriction
* in compliance with applicable auditing pronouncements
* the registered auditor has satisfied himself of the existence of all assets and liabilities shown in the financial statements (see note (b))
* proper accounting records have been kept in at least one of the official languages
* all information, vouchers and other documents which, in the registered auditor's opinion, were necessary for the proper performance of the auditor's duty, have been obtained
* the registered auditor has not had occasion to report a reportable irregularity to the Regulatory Board (see note (c))
* the registered auditor has complied with all laws relating to that entity and
* the registered auditor is satisfied as to the fairness of the financial statements.

NOTE (a): The name of the individual registered auditor responsible for the audit, must be conveyed to the client, and must be available to the Regulatory Board on request. This is an important section as it isolates responsibility and provides the IRBA with an identified individual (as opposed to the firm at large), against whom action can be taken in respect of certain offences.

NOTE (b): The use of the word "existence" in this section is not used in the narrow sense of the existence assertion only. It should be taken as meaning that the assets and liabilities shown in the financial statements are fairly presented in all respects. Of course to be in a position to satisfy this requirement, the auditor

will test all assertions applicable to the asset and liability account balances, including the disclosure assertions.

NOTE (c): Reportable irregularities are dealt with extensively in Sec 45.

2.3 In terms of Sec 44(4) and (5) and (6), if a registered auditor was responsible for keeping the books, records or accounts of an entity on which he is reporting on anything in connection with the business or financial affairs of the entity, details of the dual roles undertaken must be included in the report.

NOTE (d): In terms of Sec 90 of the Companies Act a person who alone or with a partner or employees habitually or regularly performs the duties of accountant or bookkeeper, or performs related secretarial work may ***not*** be appointed auditor.

NOTE (e): The passing of closing entries, assisting with adjusting entries or framing financial statements or other documents, are not regarded as "being responsible for keeping the books, records or accounts." (See Section 44 (5)).

NOTE (f): A registered auditor who has or has had a conflict of interest (as prescribed by the IRBA) may not conduct an audit of that entity.

3. SEC 45 – Duty to report irregularities (See Appendix "Is it an RI" on page 3/93)

This is a very important section as it places a significant responsibility on the registered auditor. The discussion which follows, is based on the section itself and advice issued to registered auditors by the IRBA.

3.1 ***Section 1 – Definitions***

In terms of the definition, a reportable irregularity means

* any unlawful act or omission committed by
* any person responsible for the management of an entity which
* has caused ***or*** is likely to cause financial loss to the entity or to its partner, member, shareholder, creditor or investor ***or***
* is fraudulent or amounts to theft ***or***
* represents a material breach of any financial duty owed by such person to the entity or any partner, member, shareholder, creditor or investor of the entity under any law applying to the entity or the conduct of management thereof.

3.2 ***Section 45 (1) and (2) – Duty to report on irregularities***

This section stipulates that the individual registered auditor (responsible and accountable for the audit) who

* is satisfied or has reason to believe that
* a reportable irregularity has taken or is taking place ***must***
* without delay
* send a written report, giving particulars of the irregularity to the Regulatory Board ***and must***
* within 3 days, notify the management board of the entity in writing, of the sending of the report, and must provide the management board with a copy of the report.

3.3 ***Section 45 (3)*** stipulates that the registered auditor must

* as soon as reasonably possible, but within 30 days of the date on which the report was sent to the Regulatory Board,
* take all reasonable measures to discuss the report with the management board of the entity

* afford the management board the opportunity to make representations in respect of the report
* send another report to the Regulatory Board, including a statement by the registered auditor that
  - ***no*** reportable irregularity has taken place or is taking place (detailed information must support this option), ***or***
  - the suspected reportable irregularity is ***no longer*** taking place and that adequate steps have been taken for the prevention or recovery of any loss, ***or***
  - the reportable irregularity is continuing.

3.4 ***Section 45 (4)*** requires that should the Regulatory Board be informed that the reportable irregularity is continuing, it must notify any appropriate regulator "as soon as possible" in writing of the details of the reportable irregularity and provide it with a copy of the report.

3.5 ***Section 45 (5)*** states that a registered auditor may carry out such investigation he deems necessary in performing any duty in terms of Sec 45.

On the face of this, it does not seem too difficult but as with most legal matters, clarity is required on a number of aspects. The following notes apply to the phrases or terms used in the definition and the section.

NOTE (a)***: Any unlawful act or omission***

* An unlawful act will be
  (i) an act which is contrary to any law passed by a government
  (ii) an act which is contrary to regulation (e.g. regulations pertaining to pollution)
  (iii) an act which is contrary to accepted common law principles.
* The unlawful act may arise out of negligence or intentionally (negligence arises where the person ought to have known that the act or omission committed, was unlawful).
* Auditors are not legal experts but, in terms of ISA250 Consideration of Laws and Regulations in an Audit of Financial Statements, should be capable of recognizing instances where non-compliance with laws and regulations by the entity may materially affect fair presentation. The auditor is not required to introduce additional audit procedures to detect unlawful acts.

NOTE (b): ***Committed by any person responsible for management of an entity***

* To be a reportable irregularity, the irregularity must have been committed by a person responsible for the management of the entity.
* For a company, this can generally be interpreted as
  (i) the board of directors of a company and the holding company in group situations, and
  (ii) any person who is a principal executive officer of the company, and
  (iii) any person who exercises executive control.
* For other types of entity, it can generally be interpreted as the
  (i) board of the entity, and
  (ii) the individuals responsible for the management of the company, and
  (iii) any person who exercises executive control.
* If an employee of an entity commits an unlawful act, ***with the knowledge or direction*** of any person responsible for management, the auditor would regard this as an unlawful act committed by management.

NOTE (c): ***Has caused or is likely to cause, material financial loss to the entity, or to any member, shareholder, creditor or investor……..***

* If the unlawful act or omission is committed by any person responsible for management, which has caused, or is likely to cause, loss to any of the above parties, it is ***reportable.***
* If the act will not cause financial loss, it is not reportable in terms of this requirement ***but*** it may still be reportable in terms of the other two conditions, i.e. the act amounts to fraud/theft or is a breach of fiduciary duty.
* Whether the loss is ***material*** is a matter of professional judgement; it does not relate to the materiality levels set for the audit. The absolute and relative size of the loss is considered, e.g. a loss of R1m as a result of an unlawful act, is in absolute terms material, but in the context of a large listed entity, it may be immaterial.
* If a benefit has been accrued from the unlawful act, it may not be set off against the "loss" incurred, e.g. a R1m bribe which results in a contract for the entity of R20m, cannot be ignored because the entity is R19m "to the good" (see note d below).

NOTE (d): ***Is fraudulent or amounts to theft***

* As indicated above, if the fraudulent act is theft or fraud but does not result in financial loss to the entity, e.g. a company submits and is paid out on a false insurance claim, the act is ***reportable*** as it is fraud. (Note: the insurance company has in fact suffered loss.)
* ***Fraud*** is defined as "the unlawful and intentional making of a misrepresentation which causes actual or potential prejudice to another", e.g. submitting a false insurance claim.
* ***Theft*** is the "unlawful taking of a thing which has value with the intention to deprive the lawful owner or the lawful possessor of that thing", e.g. members of the management team sell inventory belonging to the entity, falsify the inventory records, and keep the proceeds.

NOTE (e): ***Represents a material breach of any fiduciary duty owed by such person to the entity or any partner, member, shareholder, creditor or investor of the entity, under any law applying to the entity or the conduct or management thereof.***

* A fiduciary duty can generally be defined as an obligation to act in the best interests of another party.
* A person generally comes into a fiduciary relationship when he controls the assets of another, or holds the power to act. Fiduciaries are expected to be loyal and to act in good faith towards the person to whom they owe the fiduciary duty, and must not profit from their position as a fiduciary.
* Common examples of fiduciary relationships which the registered auditor will encounter, are
  (i) a director in relation to his company
  (ii) a member in relation to his close corporation
  (iii) a partner in relation to his co-partners
* The measurement of the ***materiality*** of the breach is again a matter of professional judgement and will bear no relationship to audit materiality. Only inconsequential or trivial breaches should be regarded as non-material.
* The key obligations in terms of the directors' fiduciary duties owed to their company, include
  (i) preventing a conflict of interest between themselves and the company
  (ii) not exceeding the limitations of their powers (ultra vires)
  (iii) considering the affairs of the company in a objective manner and in it's best interests (unfettered discretion)
  (iv) exercising their powers for the purpose for which they were granted.

NOTE (f): ***Section 45(1) and (2) place a duty on the individual registered auditor to report the irregularity***

* You will remember from Sec 44, that an ***individual registered auditor*** must be identified as responsible and accountable for an audit; it is this individual who is required to report any reportable irregularity.
* In order to report, the registered auditor does not need absolute or irrefutable proof that a reportable act has taken place; he needs only to be "satisfied or have reason to believe". If challenged, the auditor will have to show that there were sufficient grounds to report the irregularity. It is important to note that there is ***no legal protection*** for the registered auditor if he reports the irregularity ***without sufficient grounds to do so.***
* It is important to note that in respect of the reportable irregularity, the registered auditor may consider information which comes to his knowledge (or the knowledge of the firm) from any source. This will include knowledge obtained from
  (i) providing other services to an audit client, e.g. a reportable fraud is picked up whilst preparing a VAT return
  (ii) providing services to another client, e.g. at an audit of a client (company B), the auditor learns that another audit client (company A) in the same industry is paying bribes to obtain contracts
  (iii) 3rd parties, e.g. press coverage of court cases, articles about illegal importing in a particular business sector such as sports footwear.

  Obviously the auditor would be expected to consider the reliability of the source of the information.

* Using information from any source will not be regarded as a breach of the fundamental principles of ***confidentiality*** as spelled out in the Code of Professional Conduct as it is a legal requirement that the registered auditor "considers such information".

NOTE (g): ***Reporting without delay***

* From the point of "being satisfied or having reason to believe", the auditor must report "without delay." This time period is not defined and should be interpreted as the period a "reasonable auditor" would take to report.

NOTE (h): In terms of the AP Act, ***a registered auditor only has an obligation to report reportable irregularities in respect of an audit client*** (but see Note (k) below; very important!)

* In terms of section 1 – "Definitions", an audit means the examination of, in accordance with the applicable auditing standards
  (i) ***financial statements*** with the objective of expressing an opinion as to their fairness or compliance with an identified framework and any applicable statutory requirements, or
  (ii) ***financial and other information*** prepared in accordance with suitable criteria, with the objective of expressing an opinion on that financial and other information.
* Take note that the auditor has a responsibility to report in respect of an audit client, not solely in respect of the service rendered. For example : Green and Brown, a firm of registered auditors is carrying out an "agreed upon procedures" engagement for Tacksi (Pty) Ltd (no opinion is given for this type of engagement). Green and Brown also perform the annual audit of Tacksi (Pty) Ltd, and Bill Brown is the registered auditor responsible for the audit. During the course of conducting the "agreed upon procedures engagement", Gary Green the individual performing the engagement, suspects that a management fraud is taking place at Tacksi (Pty) Ltd. In terms of Green and Brown's appointment to perform agreed upon procedures, this is ***not*** a reportable irregularity, ***but*** as Tacksi (Pty) Ltd is an ***audit client***, Bill Brown should be informed of the suspected management fraud and should consider whether it is a reportable irregularity.
* It is also important to note that the definition of "audit" is not restricted to the audit of financial statements.

* Where an individual registered auditor performs an audit ***on behalf of*** the Auditor-General, "reportable irregularities" will be reported to the Auditor-General, not the IRBA. This is because the entity has not appointed the auditor, i.e. the formal relationship is between the entity and the Auditor-General.

NOTE (i): ***Reasonable measures***

* The registered auditor is required to take "reasonable measures" to discuss the report submitted to the IRBA, with the client. Most often this should be a straight-forward exercise as the client will want to discuss it. If this is not the case, reasonable measures will be judged in terms of what a reasonable auditor would do.

NOTE (j): ***Section 45(4) places a duty on the IRBA to notify any appropriate regulator in writing of the reportable irregularity.***

* The term appropriate regulator, is defined in Section 1 and covers a wide range of parties, e.g. a national government department, commissioner, regulator, authority, agency, board appointed to regulate, oversee or ensure compliance with any legislation, regulation or licence, rule, directive, notice in terms of or in compliance with, any legislation as appear appropriate to the Regulatory Board.

* Where the reportable irregularity is a criminal act, the Regulatory Board is likely to inform the Director of Public Prosecutions who may in turn request the Commercial Branch of the SAPS to investigate the matter.
  (i) if this occurs, the auditor should expect a visit from the Commercial Branch. As no legal privilege between a practitioner and a practitioner's client exists, and as the practitioner is not protected by the Code of Professional Conduct in respect of confidentiality, the practitioner cannot legally refuse to hand over documents to SAPS, provided the SAPS is acting within its powers. Legal advice should be sought immediately.

NOTE (k): In terms of the Companies Act 2008 and the Companies Regulations 2011, all companies must calculate their public interest score. This score combined with other factors, identifies certain companies which must subject their annual financial statements to an ***independent review*** by a registered auditor (chartered accountants or other categories of accountant may carry out certain reviews). As this company is not an "audit client" Sec 45 of the AP Act will not apply, so a reportable irregularity uncovered during an independent review, will ***not*** be reportable to the IRBA ***in terms of the Auditing Profession Act.*** However, in terms of Regulation 29, an independent reviewer (who will frequently be a registered auditor), will be obliged to report a "reportable irregularity" uncovered on a review engagement, but to the Commission (CIPC) not the IRBA. Requirements and procedures are essentially the same and are described in Chapter 3 of this text.

4. SEC 46 – Limitation of Liability

* Section 46 relates to liability of the registered auditor in respect of an audit conducted in accordance with the ISAs of financial statements with the objective of expressing an opinion as to their fairness in relation to an identified financial reporting framework, e.g. IFRS.
* An auditor shall, in respect of any opinion expressed or report or statement made
  (i) incur no liability to a client or third party
  (ii) unless it is proved that such opinion, report or statement was made
  (iii) maliciously, fraudulently or pursuant to a negligent performance of the auditor's duties.
* Where it is proved that such opinion, report or statement was given pursuant to a negligent performance, the auditor will only be liable to ***3rd parties*** if it is proved that at the time of the negligent performance, the registered auditor ***knew or could reasonably have been expected to know*** that
  (i) his client would use the opinion to induce a 3rd party to act or refrain from acting, ***or*** that

(ii) the 3rd party would rely on the opinion for the purpose of acting or refraining from acting in some way.

NOTE (a): If after the opinion was given, the registered auditor represented to a 3rd party that it was correct, while at the same time he knew or could reasonably have been expected to know that the 3rd party would rely on the opinion, he will be liable if the 3rd party suffers loss as a result of the reliance on the negligently given opinion.

NOTE (b): The mere fact that a registered auditor performed the duties of auditor, shall not in itself be proof that he "could reasonably have been expected to know". In other words, just because you are the auditor, does not mean that you are expected to know or be able to foresee who might rely on the audit opinion and under what circumstances the reliance might occur.

NOTE (c): A registered auditor's liability hinges around ***negligent*** performance by the auditor. As can be seen in Section 46(2), the auditor can incur no liability to ***client*** or ***3rd party, unless*** it is proved that the opinion, report or statement was given maliciously (the vast majority of auditors do not act maliciously) or fraudulently, pursuant to a negligent performance.

NOTE (d): A distinction must be drawn between liability to ***clients*** and liability to ***3rd parties.***

An auditor's liability to ***clients*** is based upon breach of contract or delict, i.e. the client could sue the auditor for financial loss on the grounds that the auditor did not meet the terms of the engagement (contract) or in delict on the grounds that the auditor did not meet his "duty of care".

An auditor's liability to ***3rd parties cannot*** be based upon breach of contract as there is normally no contract between the auditor and the 3rd party, i.e. the auditor "contracts" with his client, not with the parties who may use the audited financial statements. The 3rd party will therefore have to bring a delictual action against the auditor and prove that :

* the auditor was negligent in expressing the opinion, or making his report or statement
* the 3rd party relied upon the opinion, report or statement and
* suffered loss as a result of the reliance and
* that the auditor knew or reasonably could have been expected to know (at the time the negligence occurred) that
* the third party would rely on the opinion, report or statement.

NOTE (e): The most important consideration is, ***how is negligence proved***? The basis of the answer is provided by the following :

"A court of law, when considering the adequacy of the work of an auditor, is likely to seek confirmation that in the performance of his or her work, the auditor has in all material respects, complied with the statements on auditing standards. In the event of significant deviation from the guidance on specific matters contained in the statements on auditing standards, the auditor may be required to demonstrate that such deviation did not result in failure to achieve the generally accepted auditing standards."

The auditing statements in effect provide the standards to which the registered auditor must adhere in the performance of his function. It stands to reason therefore, that if the performance of the auditor is to be judged, it will be judged against the standards which the profession itself has set.

The impact of reportable irregularities on the audit opinion

1. A reportable irregularity may or may not have an affect on fair presentation of the financial statements.
   * If the reportable irregularity ***does*** affect fair presentation then the auditor must qualify the report in accordance with ISA 705, Modifications to the opinion in the Independent Auditor's Report.
   * If the reportable irregularity does ***not*** affect fair presentation (but nevertheless exists), the audit report must be modified by the inclusion of an additional paragraph in the audit report. This paragraph would be headed "Report on Other Legal and Regulatory Requirements" and is similar to an emphasis of matter paragraph. Note that even where the reportable irregularity existed but has been rectified/resolved, it cannot be ignored for audit reporting purposes. Refer to Chapter 18, The Audit Report for further discussion.
   * If a matter which the auditor reported to the IRBA as a reportable irregularity, turns out ***not*** to be a reportable irregularity, then no mention of the matter should be made in the audit report.

Consequences for the individual registered auditor for failing to report a reportable irregularity

1. These can be severe. In the first instance, the individual registered auditor may face investigation and disciplinary action by the IRBA in terms of Sections 48, 49 and 50. This would amount to an investigation into improper conduct and could result in the punishments described in Chapter V Sec 51. See below.

2. In addition, the individual registered auditor, or the firm, may face a civil claim for damages brought by aggrieved parties, e.g. someone who suffered loss as a result of the auditor failing to report the irregularity.

3. In terms of Section 52, which deals with the failure to report a reportable irregularity, a registered auditor may face criminal charges which could result in a jail term not exceeding 10 years, and/or a fine. Criminal charges are complicated, but simplistically stated, if a registered auditor is satisfied that a reportable irregularity exists, but intentionally/deliberately does not pursue it, he may face criminal charges.

CHAPTER V – ACCOUNTABILITY OF REGISTERED AUDITORS (Sections 47 to 51)

This chapter gives the IRBA the powers to inspect or review the practice of a registered auditor (Sec 47), investigate a charge of improper conduct against a registered auditor (Sec 48), formally charge a registered auditor with improper conduct if necessary (Sec 49), and proceed with a formal disciplinary hearing (Sec 50). It also lays down the procedure to be followed after the disciplinary hearing and identifies the categories of punishment which may be given (Sec 51). The punishments are

* a caution or reprimand
* a fine
* suspension of the right to practice for a specified period or
* cancellation of the registered auditors registration, and his removal from the register
* a combination of the above.

CHAPTER VI – OFFENCES (Section 52)

1. ***SEC 52 – reportable irregularities and false statements in connection with audits***

   This section, the only section in Chapter VI, states that a registered auditor who
   * fails to report a reportable irregularity, or
   * knowingly or recklessly expresses an opinion or makes a report or other statement which is false in a material respect, shall be guilty of an offence.

NOTE (a): A registered auditor convicted in a court of law under this section, is liable to a fine or imprisonment of up to 10 years, or both.

NOTE (b): For a criminal conviction to be obtained against a registered auditor for failing to report a reportable irregularity, he must have intentionally/deliberately not reported it.

CHAPTER VII – GENERAL MATTERS (Sections 55 to 60)

This chapter consists of six sections, none of which are particularly pertinent to academic study. The Chapter deals with the powers of the Minister of Finance (Sec 55), Indemnity (Sec 56), Administrative matters (Sec 57), Repeal and amendment of laws (Sec 58), and Transitional matters (Sec 59). This section facilitated the transition of the former Public Accountants' and Auditors' Board to the Independent Regulatory Board for Auditors (IRBA). The final section in the Act is Section 60 which states that the name of the Act will be the "Auditing Profession Act 2005".

APPENDIX - IS IT A REPORTABLE IRREGULARITY? – 10 QUESTIONS

1	***Is (was) the act committed by a person(s) responsible for management of the entity?***	Yes	Proceed to question 2
		No	No reportable irregularity exists – nothing further to be done
2	***Is the act an unlawful act or omission?***	Yes	Proceed to question 3
		No	No reportable irregularity exists – nothing further to be done
3	***Does the act result in material financial loss?***	Yes	Yes to Q1, Q2, Q3 means that an RI exists
		No	Consider question 4
4	***Is the act fraud or theft?***	Yes	Proceed. Yes to Q1, Q2 and Q4 means that an RI exists
		No	Consider question 5
5	***Is the act a material breach of fiduciary duty?***	Yes	Proceed. Yes to Q1, Q2 and Q5 means that an RI exists.
		No	No reportable irregularity exists if the answers to Q3, Q4 and Q5 are also No
6	***Must the matter be reported to the IRBA?***	Yes	If the answers to Q1, Q2 and any of Q3, Q4, or Q5 is yes
7	***When must the 1st report be made to the IRBA?***		"Without delay" from when the auditor is satisfied or has reason to believe that a reportable irregularity has taken place
8	***When must management be notified of the report?***		Within 3 days of the auditor making the 1st report to the IRBA
9	***What must the auditor do next?***		Take all reasonable steps to discuss the report with management and having done so must make a 2nd report to IRBA which states that 9.1 ***no*** reportable irregularity has or is taking place ***or*** 9.2 the suspected reportable irregularity is no longer taking place ***and*** that adequate steps have been taken for the prevention or recovery of any loss ***or*** 9.3 that the reportable irregularity is continuing
10	***Is there a time limit on this 2nd report?***	Yes	As soon as reasonably possible but no later than 30 days from the date of the 1st report to the IRBA.

CHAPTER 4

CORPORATE GOVERNANCE

CONTENTS

			Page
INTRODUCTION			4/3
BRIEF BACKGROUND TO CORPORATE GOVERNANCE IN SOUTH AFRICA			4/3
KING III – CODE OF GOVERNANCE PRINCIPLES			4/4
1.	Basis of the Code		4/4
2.	"Apply or Explain" and the law		4/5
3.	Key aspects of the King III report		4/5
4.	Sustainability		4/6
5.	Important issues incorporated into the report		4/6
6.	Application of the Code		4/7
THE CODE OF GOVERNANCE PRINCIPLES			4/7
Topic 1 – Ethical leadership and corporate citizenship			4/7
Element	-	Responsible leadership, the board's responsibilities and ethical foundation	4/7
Topic 2 – Boards and Directors			4/9
Element	-	Role and Function of the board	4/9
	-	Composition of the board	4/12
	-	Board appointment process	4/13
	-	Director development	4/13
	-	Company Secretary	4/14
	-	Performance assessment	4/14
	-	Board committees	4/15
	-	Group boards	4/15
	-	Remuneration of directors and senior executives	4/16
Topic 3 – Audit Committees			4/17
Element	-	Existence of audit committees	4/17
	-	Membership and resources of the audit committee	4/17
	-	Responsibilities of the audit committee	4/18
	-	Internal assurance providers	4/19
	-	External assurance providers	4/21
	-	Reporting	4/21
Topic 4 – The governance of risk			4/21
Element	-	The board's responsibility for risk governance	4/21
	-	Management's responsibility for risk management	4/23
	-	Risk assessment	4/23
	-	Risk response	4/25
	-	Risk monitoring	4/25
	-	Risk assurance	4/26
	-	Risk disclosure	4/26
Topic 5 – The governance of information technology			4/26
Element	-	The board's responsibility for IT governance	4/26

Topic 6 – Compliance with laws, rules, codes and standards 4/29
Element - Companies, boards and individual directors 4/29

Topic 7 – Internal Audit 4/30
Element - The need for and role of internal audit 4/30
- Internal audit's approach and plan 4/30
- Internal audit's status in the company 4/31

Topic 8 – Governing stakeholder relationships 4/32
Element - Stakeholders and the company 4/32
- Dispute resolution 4/36

Topic 9 – Integrated reporting and disclosure 4/37
Element - Transparency and accountability 4/37

INTRODUCTION

Companies are an integral part of modern society. We are all linked in numerous ways to companies. The goods we purchase are, more often than not, produced by companies, many people are employed by companies, and the public invests in companies whether it be through pension funds, unit trusts or direct shareholdings. Our leisure activities are often supported by companies through advertising and sponsorship and many public facilities are paid for by the taxes which companies contribute to the government. It follows therefore that healthy, honest, open, competently and responsibly controlled companies will improve the quality of modern society.

Whilst conceding that the interests of society at large are very important, it must not be forgotten that some members of society have a more direct relationship with a company. This would include the shareholders, employees, providers of finance, and groupings with which the company "does business" such as the company's suppliers. The challenge therefore, is to run companies within a framework which satisfies the needs of all stakeholders. For example, a shareholder will probably be intent on maximising his return on investment, whilst a supplier will require that his account be paid promptly and that he can continue to sell his products to the company. An employee might look for fair terms of employment, whilst the general public may be more concerned about pollution control in their neighbourhood if it is located near an oil refinery.

So what is corporate governance? - It is the system or process whereby companies are directed or controlled. It is about companies being good corporate citizens and all that that entails.

BRIEF BACKGROUND TO CORPORATE GOVERNANCE IN SOUTH AFRICA

1. The King Report 1994

Whilst many companies have embraced good corporate governance for many years, it was only in 1994 that the King Report on Corporate Governance was issued. This Report "formalised" an approach to corporate governance by recommending a Code of Corporate Practices and Conduct to be adopted by "big business". The JSE made it a requirement for all companies listed on the exchange to include, in their annual financial statements, a statement by the directors on their compliance with the Code.

2. Effect of the King Report 1994

It would be a gross exaggeration to state that the King Report had a dramatic effect on business ethics and morality in South Africa, or that companies suddenly embraced the principles of ***openness, integrity and accountability*** as advocated in the Report. This is clearly evidenced by the number of high profile financial scandals, corporate failures and dishonest conduct by company directors that have been blazoned across both the financial and popular press. At the same time however, it must be acknowledged that the King Report started to get "things rolling," to bring a level of consciousness to the general public and the financial world that companies have an accountability and responsibility to a wider front. Indeed, without the King Report, many of the scandals etc, referred to above, may not have received the coverage they did!

3. The King Report 2002

The 1994 King Report was followed by the 2002 King Report (frequently referred to as King II). A committee was constituted under the chairmanship of Mervyn King S.C. to primarily "review the King Report 1994 and to assess its currency against developments, locally and internationally, since its publication in 1994" and to "consider and recommend reporting on issues associated with social and ethical accounting, auditing and reporting on safety, health and environment". The committee also sought to recommend how the success of a company's compliance with a new Code of Corporate Governance could be measured.

The King Committee consisted of representatives from all major interest groups, including the internal and external audit professions. The report was issued in March 2002, effective in respect of affected companies whose financial years commenced on or after 1 March 2002. The product of the 2002 King Report was the Code of Corporate Practices and Conduct. This was a set of principles/recommendations not a prescriptive set of instructions or an Act. It did not in any way

supersede laws and regulations pertaining to companies or business in general and did not lay down a set of "punishments" for breaches of the Code. As with King I, the JSE required compliance with the recommendations of King II by listed companies.

4. Developments in legislation

During the period between the issue of King II (2002) and King III (2009) the new Auditing Profession Act 2005 and The Corporate Laws Amendment Act 2006 were promulgated. Both of these Acts contained sections designed to strengthen and support good corporate governance. These Acts were both part of the larger "corporate reform" initiative which culminated in the promulgation of the Companies Act 2008. This Act places significant emphasis on corporate governance.

KING III – CODE OF GOVERNANCE PRINCIPLES (effective March 2010)

This chapter is based upon the "Code of Governance Principles" developed under the auspices of the Institute of Directors in Southern Africa.

Corporate governance is not static. It must evolve to meet and shape developments in business and society, and hence the need for the third King Report. The primary reasons for King III were

* the promulgation of the Companies Act 2008 and
* changes in international trends.

Many of the ideas, principles and characteristics of good governance developed in King I and King II remain in King III; some have been re-expressed and some have been added. The following points of discussion are necessary for a sound understanding and appreciation of the code.

1. Basis of the Code

1.1 The basis of any "code" on corporate governance can be legislated (a set of rules), or voluntary (principles and practices) or a combination of both. Essentially the legislated basis is the "big stick" approach which lays down rules to which companies, directors etc must adhere, and punishments which will be meted out if the rules are broken. The voluntary approach presents companies, directors, etc with a set of principles and best practice in an attempt to get companies and directors to voluntarily adopt these principles and best practice because it is the best way to go for the company and society. A combination of the two is obvious, some matters of governance are legislated, e.g. public companies must be externally audited and must have an audit committee, and other matters are expressed in principle, e.g. the board must show leadership and the company should be a good corporate citizen.

1.2 The King III Code identifies these two bases as "comply or else" or "comply or explain" and describes a variation of the latter, i.e. "apply or explain".

- "***comply or else***" conveys that companies etc must adhere to the rules and if they don't, they will be punished.
- "***comply or explain***" conveys that the principles and practices recommended by the Code should be the focus of the company's corporate governance. However, if the directors consider that compliance with a particular recommendation is not in the best interests of the company then the directors are at liberty not to comply but must explain the reason behind their decision.
- ***"apply or explain"*** as indicated above, "apply or explain" is simply a variation of the "comply or explain" basis. In the opinion of the King III committee (and other similar international bodies), the word "comply" is too strong and inflexible. Using the word "apply" suggests a more accommodating approach. Thus King III is on the "apply or explain" basis. From a practical point of view this means:

  > "in following the "apply or explain" basis, the board of directors, in it's collective decision making, could conclude that to follow a recommendation would not, in the particular circumstances, be in the best interests of the company. The board could decide to apply the recommendation differently or apply another practice and still achieve the objective of the corporate governance principles of fairness, accountability, responsibility and transparency. Explaining how the principles

and recommendations were applied, or if not applied, the reasons, results in compliance."

Adopting the "apply or explain" basis will hopefully generate a culture of good corporate governance in which companies and directors etc willingly embrace best practice rather than being forced into it.

2. "Apply or explain" and the law

2.1 The "apply or explain" basis does not mean that corporate governance and the law can be separated. As the term suggests, corporate governance is about governing companies. This is achieved by the directors of the company putting in structures, processes and procedures which achieve the objectives of the company but within the framework of the law. As a starting point, the directors themselves have legal duties.

- They are obliged to act with a duty of care, skill and diligence in managing the business and
- They have a fiduciary duty to act in the best interests of the company, to avoid conflicts, and not to make secret profits.

If they fail in these fundamental duties they can be found guilty of gross negligence, misconduct or breach of trust.

2.2 As has been mentioned earlier, the Companies Act 2008 requires that public companies and state owned enterprises be audited and that they appoint audit committees. In fulfilling their duties, the directors must ensure that this happens, they cannot decide not to have an audit because it is inconvenient or costs too much!

2.3 The Act also makes certain individuals ineligible for appointment as a director such as a person convicted and imprisoned for theft, forgery or fraud; directors must declare their financial interest in any matter to be considered at a meeting of the board and as a final example, directors must produce financial statements (i.e. report their performance) to stakeholders. These legal requirements, all related to governance, must be complied with.

2.4 The purpose of these paragraphs is to illustrate that corporate governance and the law are intertwined. The "apply or explain" basis does not allow directors to break the law and then justify doing so by claiming it was in the best interests of the company. However, where the directors have chosen ***not*** to adopt a ***governance recommendation***, the "apply or explain" basis provides them with the opportunity of achieving compliance by providing an explanation.

3. Key aspects of the King III report

3.1 ***Leadership*** – good governance is about effective leadership. Leadership is characterized by the ethical values of responsibility, accountability, fairness and transparency and is based on moral duties that find expression in the concept of Ubuntu (humaneness, mutual support and respect, interdependence, unity, collective work and responsibility).

3.2 ***Sustainability*** – to understand the term "sustainability" we need to understand that companies do not operate in a vacuum, they are part and parcel of society and must address, and be part of, the social, ethical and environmental issues which arise out of society. Should a company fail to understand and react to its position in society, the implication is that it will not survive i.e. it is not ***sustainable***. There is no sustainability or future for companies which ravage the environment or exploit their constituency.

3.3 ***Corporate citizenship*** – the concept of corporate citizenship flows from the fact that the company is a person and should operate in a sustainable manner. The concept implies an ethical relationship of responsibility between the company and the society in which it operates. Companies have rights but also legal and moral obligations in respect of their economic, social and natural environments.

4. Sustainability

Sustainability is regarded as the primary moral and economic imperative of the 21st century and King III considers that a key challenge for companies is to make sustainability issues mainstream, to the extent that governance, strategy and sustainability are inseparable. Central to this theme is the requirement that companies perform in a manner which is sustainable ***and*** that they report to their stakeholders on their sustainability. By issuing integrated sustainability reports, a company increases the trust and confidence of its stakeholders and the legitimacy of its operations. The important aspects of sustainability are:

4.1 ***Inclusivity of stakeholders*** – to achieve sustainability, the legitimate interests and expectations of ***all*** stakeholders must be taken into account in decision making and strategy. Stakeholders will include, employees, suppliers, the community in which the company operates, investors, customers, etc.

4.2 ***Innovation, fairness and collaboration*** – these are key aspects in achieving sustainability. Innovation provides new ways of achieving sustainability, fairness is vital because social injustice is unsustainable and collaboration (and co-operation) is required if business at large is going to embrace the principles of sound corporate governance proposed by King III.

4.3 ***Social transformation*** – to achieve (move towards greater) sustainability, social transformation must be part and parcel of a company's performance. This will provide benefits for both company and society. However, it does not mean making a token gesture to a community and then sitting back; it means developing a long-term achievable strategy to uplift that community.

None of the above should be interpreted to mean that companies should not be in business to make profits – a company that does not make a profit is not sustainable – but there is much more to running a company than making a profit.

5. Important issues incorporated into the King III report

5.1 ***Alternative dispute resolution (ADR)*** – It is an emerging trend in international business, that where disputes arise in business dealings, mediation/arbitration ***as opposed to going to court*** is an acceptable way of resolving the dispute. From a governance perspective, where a dispute arises, it is a duty of the directors to resolve the dispute timeously, efficiently and effectively. ADR clauses are now frequently included in contracts and mediation and arbitration should be regarded as "good governance".

The Companies Act 2008 Sec 166 underscores this acceptance of ADR as a sound mechanism by providing a person seeking relief in terms of the Companies Act, to apply for alternative dispute resolution rather than applying to the court.

5.2 ***Risk-based internal audit*** – King III favours risk based internal audit over compliance based internal audit. The compliance based approach has internal audit checking that the company has complied with its internal controls, legislation etc. The risk-based approach places more emphasis on internal audit understanding the risks associated with the strategic direction of the company and determining whether internal controls, processes and procedures, adequately address these risks.

5.3 ***IT governance*** - If you think about the international banking system, electronic banking, use of the internet by businesses, it is very easy to understand that issues such as confidentiality, integrity, functionality of the system are of paramount importance in the management of the company. Again the directors have significant responsibility with regard to IT governance. If this is not met, the sustainability of the company is at severe risk.

5.4 ***Business rescue -*** Rescuing a business means that the business has been sustained, and is clearly in the interests of all the business's stakeholders. The Companies Act 2008 has introduced legislation relating to business rescue and King III has made complementary recommendations.

6. Application of the Code

Unlike King I and King II, King III has not stipulated specific companies to which King III applies, stating that it "applies to all entities regardless of the manner and form of incorporation". Obviously the size and nature of the company will determine how the entity applies the recommendations, and it is recommended by King III that all entities disclose which principles and/or practices they have decided not to apply and explain why.

THE CODE OF GOVERNANCE PRINCIPLES

The Code of Governance Principles deals with a number of separate (but interrelated) ***topics*** e.g. Boards and Directors, Audit Committees, Risk Management etc. Each topic is broken down into ***governance elements*** and a series of ***principles*** are attached to each element. Each principle has a number of recommended practices attached to it,

e.g. ***Topic***: Boards and Directors
Governance Element: Role and function of the Board.
Principle: The board should act as the focal point for, and custodian of, corporate governance.
Recommended Practice: The board should have a charter laying out its responsibilities.

This chapter will attempt to present the principles and summarise what they entail to the extent necessary for students to understand "corporate governance". All "topics" will be covered and all "governance elements" and principles will be included. Recommended practice will be discussed as appropriate.

1. TOPIC 1: ETHICAL LEADERSHIP AND CORPORATE CITIZENSHIP

Element: Responsible leadership, the board's responsibilities and ethical foundation

Principle 1.1: The board should provide effective leadership based on an ethical foundation.

1.1.1 If the board is to satisfy this principle, it must direct the strategy and operations of the business towards building a sustainable business.

1.1.2 The strategy adopted should take into account the long and short terms impact of the strategy on the ***economy, society*** and the ***environment***.

1.1.3 The board should set its ethical values in a code of conduct and ensure that the conduct of management (and other employees) is aligned to these values.

1.1.4 King III, in following the precedent set by King I and II, has adopted the stakeholder approach (or stakeholder model) to corporate governance which emphasizes that the board is answerable to all of the stakeholders of the company ***not*** just the company and/or its shareholders.

1.1.5 All aspects of corporate governance are based on ethical values and standards, and the ethics of governance require that all decisions and actions of the board be based on four ethical values.

* ***Responsibility*** - the board should assume responsibility for the assets and actions of the company and should take corrective action to keep the company on its correct path.

* ***Accountability*** - the board should be able to justify its decisions and actions to all stakeholders.

* ***Fairness*** - in its decisions and actions, the board should ensure it gives fair consideration to the interests of all stakeholders.

* ***Transparency*** - the board should disclose information in a manner that enables all stakeholders to make informed analysis of the company's performance.

With regard to a director, the ethics of governance require that each director adhere to these four basic ethical values ***and*** that each director exercise the following moral duties

* ***conscience*** - a director should act with intellectual honesty, in the best interest of the company, avoid conflicts of interest and remain independent in mind and action.
* ***care*** - a director should pay careful attention to the affairs of the company, a carefree or careless attitude is not acceptable.
* ***competence*** - a director should have the necessary knowledge and skills to exercise his duties and should continuously "upgrade" knowledge, e.g. keep abreast with IT development.
* ***commitment*** - a director should be diligent and prepared to put in the necessary time and effort.
* ***courage*** - a director should have the courage to take the risks associated with "directing and controlling" a company ***and*** should have the courage to act with integrity, even when there is pressure on him to act otherwise, or be unpopular.

Principle 1.2: The board should ensure that the company is, and is seen to be, a responsible corporate citizen.

1.2.1 The success of the company should not only be judged in terms of the financial performance of the company, but also in terms of the impact of the company on the economy, society and the environment.

1.2.2 The company should protect, enhance and invest in the well being of the economy, society and the environment.

1.2.3 With regard to its dealings with stakeholders, the company should:
* be guided by the Constitution and Bill of Rights
* promote ethical conduct collaboratively
* develop measurable corporate citizenship programmes.

1.2.4 Being a good citizen for a company, means the establishment of an ethical relationship of responsibility between the company and the society in which it operates. Companies have rights, but they also have legal and moral obligations in respect of their social and natural environments.

1.2.5 Being a good corporate citizen and sustainability are inseparable; the good corporate citizen will endeavour to infuse good governance and sustainability into all aspects of the business, i.e.
* managing the enterprise – how effectively and ethically the company governs, controls and manages its operation
* workplace practices – how it manages its employees, workplace conditions and employment practices
* stakeholder interactions – how it engages external stakeholders in the company supply chain, market place, government and community
* environment – how it controls its impact on the environment and
* transformation – how SA companies meet their obligations to help all citizens become meaningful, economic partners.

1.2.6 A very important aspect is "stakeholder interaction" and a significant part of this is the concept of the company reporting on its ***triple bottom line***, that is, the company's economic, social and environmental performance
* the ***economic*** aspect relates to the financial and non-financial information relevant to the company's business
* the ***environmental*** aspect includes the effect of the company's activities, products and services on the environment
* the ***social*** aspect embraces the values, ethics and relationships with the stakeholders of the company which the company promotes.

In addition to the value of the information to stakeholders, embracing the "triple bottom line" concept will focus companies on the governance and sustainability requirements of being a good corporate citizen.

1.2.7 There is no simple universal approach to "good citizen" programmes. In any event, good citizen programmes are only a part of being a good corporate citizen. However, there should be tangible programmes which focus on the needs of the country, e.g. transformation, human rights, health (HIV/AIDS), housing, etc.

1.2.8 Results of good citizen programmes should be measurable and reportable.

1.2.9 Being a good corporate citizen is far more than projecting an image and getting public relations right. It is about genuine commitment and leadership in the company, not a series of publicity stunts or a passing phase.

Principle 1.3: The board should ensure that the company's ethics are managed effectively.

1.3.1 The board is responsible for creating and sustaining ethical corporate culture in the company. An ethical corporate culture requires that

* ethical practice for directors is a non-negotiable requirement
* sound moral values and ethics are propagated by the conduct of individuals (throughout the company)
* business activity is directed by people with integrity, fairness, responsibility and vision
* laws and regulations are obeyed; unfair practices, abuse of economic power (unfair treatment of suppliers) and collusion (e.g. price fixing) are avoided
* "having to be ethical" cannot be used as an excuse for poor business performance
* the director's duty is firstly to his company and shareholders, but the interests of ***all*** stakeholders must be considered.

1.3.2 Creating an ethical corporate culture requires that the company has a well designed and properly implemented ethics management process consisting of the following four aspects

* ***Compilation of an ethics, risks and opportunity profile.*** An ethical risk would be doing business in a country/sector where bribery is rife. An ethical opportunity would be entering a business arrangement with a company with a well known reputation for ethical conduct.
* ***Development of a Code of Ethics*** which lays down ethical values, standards and specific guidelines for the company in its dealing with internal and external stakeholders.
* ***Integration of ethics*** into the company's strategies and operations. This will include, ethical leadership, education and training for employees, communication of ethical requirements and advice on ethical issues which may arise, and the prevention and detection of misconduct e.g. by whistle blowing.
* ***Ethics performance reporting and disclosure***. The board should assess the company's ethical performance and disclose findings to internal and external stakeholders, in the integrated report.

2. TOPIC 2: BOARDS AND DIRECTORS

Element: Role and Function of the Board.

Principle 2.1: The board should act as the focal point for and custodian of corporate governance.

2.1.1 This means that the company should exercise leadership, integrity and judgement to achieve prosperity and sustainability. It should

* have a charter laying out its responsibilities
* meet at least four times a year
* monitor the relationship between management and the stakeholders of the company.

Principle 2.2: The board should appreciate that strategy, risk, performance and sustainability are inseparable.

2.2.1 The board should take responsibility in developing and approving the short and long-term strategies of the company. It should not allow management to decide on strategy and get on with it as they deem fit. In setting strategy, the board must identify key performance and risk areas and set objectives that are clear, measurable, profitable and ***sustainable***, taking into account "people, planet and profit".

2.2.2 The strategy of the company must be aligned to the legitimate interests and expectations of its stakeholders, and risks must be thoroughly evaluated.

2.2.3 Sustainability is about keeping the company going in the long-term, i.e. it is about the going concern ability of the company.

2.2.4 Numerous conditions and events can threaten the sustainability of a company and they are as diverse as the activities in which companies are engaged. For example

* how does a company which sells music compact discs and DVDs address the sustainability of its business in the face of the availability of internet downloads?
* how does a company making its money from a scarce resource, e.g. oil, minerals, etc, sustain itself?
* in the shorter term, how does a company respond to the risk of a lack of skills in its business, e.g. a shortage of suitable scientists?
* how does a company highly dependent on efficient IT technology, e.g. a bank, ensure that it meets customer expectations?

2.2.5 The point is that sustainability issues have a significant effect on the economic value of a company and thus failure to identify, respond to and monitor these risks will spell the end of the company.

Principles 2.3, 2.4 and 2.5 are repeats of the principles of ethical leadership: They are dealt with under topic 1.

Principle 2.6: The board should ensure the company has an effective and independent audit committee. This is dealt with under topic 3.

Principle 2.7: The board should be responsible for the governance of risk. This is dealt with under topic 4.

Principle 2.8: The board should be responsible for information technology (IT) governance. This is dealt with under topic 5.

Principle 2.9: The board should ensure that the company complies with applicable laws and considers adherence to non-binding rules, codes and standards. This is dealt with under topic 6.

Principle 2.10: The board should ensure that there is effective risk-based internal audit. This is dealt with under topic 7.

Principle 2.11: The board should appreciate that stakeholders' perceptions affect the company's reputation.

2.11.1 A good reputation provides many benefits for a company. For example, they can attract better candidates for employment, have better relationships with their stakeholders, attract business ventures with other companies with good reputations and often enjoy free advertising from positive media coverage.

2.11.2 On the other hand, business reputations can be tarnished very easily. Corporate scandals, rumour mongering, internal conflicts made public, unethical behaviour by employees who interact with the public and a host of other situations, can undo a good reputation.

2.11.3 It is therefore imperative that a good reputation be seen as an "asset" to be protected. Reputational damage is regarded as one of the major risks facing the modern company and the board should ensure that there is a process of measuring, monitoring and managing reputation assets and liabilities (factors which may be adversely affecting the company's reputation).

2.11.4 Risks to a company's reputation do not arise in isolation. Many decisions taken by a company have the potential to damage (or enhance) a company's reputation and the risk assessment process must realize this. For example, the decision by a company to discontinue its HIV/AIDS treatment programme for its employees may damage its reputation in the eyes of its customer base.

2.11.5 This principle is further dealt with under topic 8.

Principle 2.12: The board should ensure the integrity of the company's integrated report. This is dealt with under topic 9.

Principle 2.13: The board should report on the effectiveness of the company's system of internal controls. This is dealt with under topics 7 and 9.

Principle 2.14: The board and its directors should act in the best interests of the company.

2.14.1 This is a fundamental principle in law. In terms of the Companies Act 2008, Sec 76, a director
* must not use the position of the director to gain an advantage for himself, or knowingly cause harm to the company.
* must exercise his powers in good faith and for a proper purpose in the best interests of the company
* must act with the degree of care, skill and diligence that may reasonably be expected of a person
  - carrying out the same functions in relation to the company as those carried out by that director, and
  - having the general knowledge, skill and experience of that director.

2.14.2 A director has an overriding fiduciary duty to act in good faith, in a manner that the director reasonably believes is in the best interests of the company, and in terms of the common law, may be held liable for loss, damages or costs of any breach of this duty.

2.14.3 The personal interests of a director or a person closely associated with the director, should not take precedence over those of the company. This principle has been partially legislated for by Sec 75 of the Companies Act 2008, which requires that a director disclose any financial interest which he may have (or which any person related to the director, as defined by Sec 2, may have) in any matter which is to be considered at a meeting of the board. For example, the board may be considering entering into a contract with a company owned by a director's wife (related person). The director must declare this fact before the meeting and should not take part in the "consideration" or approval of the matter.

2.14.4 Conflicts of interest may not be as clear cut as this example and may only be known to the director himself. It is up to the director's integrity to do the right thing, e.g. declare the conflict, resign from the board, whatever is appropriate. King III does recommend that all listed companies have a policy relating to their directors, officers and other selected employees dealing in the shares of the company.

Principle 2.15: The board should consider business rescue proceedings or other turnaround mechanisms as soon as the company is financially distressed as defined in the Companies Act.

2.15.1 Chapter 6 of the Companies Act 2008 deals extensively with business rescue. From a governance perspective it is the duty of the directors to "sustain" the company, and entering into business rescue arrangements may be an option when
* the company is financially distressed and
* there appears to be a reasonable prospect that the company can be rescued.

2.15.2 The board should take particular notice of Sec 22 of the Companies Act 2008, which states that a company must not carry on its business recklessly or with gross negligence. A company which is financially distressed may be vulnerable to breaches of this section.

2.15.3 The board should continuously monitor the solvency and liquidity of the company.

Principle 2.16: The board should elect a chairman who is an independent non-executive director. The CEO of the company should not also fulfil the role of chairman of the board.

2.16.1 The chairman should be
* appointed on an annual basis
* independent and not conflicted (the appointment of a chairman who is not independent should be justified in the integrated report).

2.16.2 The role of the chairman should be formalized, and his ability to add value, and his performance against what is expected of his role and function should be assessed annually, as should his independence.

2.16.3 The chairman should focus on social, sustainability and transformation issues including employment equity, diversity management and social investment.

2.16.4 The board should have a succession plan in place for the position of chairman. Any former CEO of the company should not be eligible for appointment as chairman until three years have elapsed.

2.16.5 The chairman and board should consider the number of chairmanships held by the chairman with a view to satisfying themselves that the role of chairman is appropriately executed.

2.16.6 The chairman should
* ***not*** be a member of the audit committee
* ***not*** chair the remuneration committee (may be a member)
* ***not*** chair the risk committee (may be a member)
* be a member of the nomination committee and may chair it.

2.16.7 Where the board appoints a chairman who does not meet all the "independence" or "non-executive" requirements, the company should be able to justify its decision and should appoint a "Lead independent non-executive director". Obviously the LID must satisfy all of the "independence" and "non-executive" requirements. The LID's role is to provide leadership and advice to the board, particularly where the chairman has a conflict of interest arising from the fact that he is not truly independent.

Principle 2.17: The board should appoint the chief executive officer and establish a framework for the delegation of authority.

2.17.1 The board should appoint the CEO and provide input into the appointment of senior management.

2.17.2 The role of the CEO should be formalized and the performance of the CEO evaluated against specified criteria.

2.17.3 The board should ensure that there is a succession plan in place for the CEO and other senior executives.

2.17.4 The CEO is central to the sustainability of the company and should
* play a critical and strategic role in the operation of the company
* ensure that the long-term strategy and vision of the company is developed and implemented
* ensure that a positive and ethical work climate is maintained
* foster a corporate culture that promotes sustainable ethical practices, encourages individual integrity and fulfils social responsibility objectives.

2.17.5 The CEO should
* not be the chairman
* not be a member of the ***remuneration, audit*** or ***nomination*** committees, but should attend by invitation, recusing himself when matters of personal interest arise
* not take on the chairmanship of ***other*** companies (outside the group)
* consider carefully the appropriateness of taking on non-executive directorships in other companies outside the group.

Element: Composition of the Board

Principle 2.18: The board should comprise a balance of power with a majority of non-executive directors. The majority of non-executive directors should be independent.

2.18.1 ***Executive director:***
* a director who is involved in the management of the company and/or is a full-time salaried employee of the company and/or its subsidiary
* an executive director of a company may also be a non-executive director of another company, provided it is not detrimental to his responsibilities as an executive director. Such a non-executive appointment should be in accordance with a board approved policy, and the chairman and chief executive officer should be consulted on the appropriateness of the policy.

2.18.2 ***Non-executive director:***
* a director who is ***not*** involved in the management of the company.

The role of the non-executive director is to provide ***independent*** judgment and advice/opinion on issues facing the company. They are required to attend board and board committee meetings and maintain a broad knowledge of the economic environment, industry and business of the company.

Non-executive directors have a duty of care, skill and diligence and should not take on more directorships than they can properly deal with.

2.18.3 ***Independent non-executive director:***
a director who

* is not a representative of a shareholder who has the ability to control or significantly influence management
* does not have a direct or indirect interest in the company (including its holding or subsidiary company) which is material to the director or the company. (A holding of 5% or more is considered material)
* has not been employed by the company (or group) in any executive capacity for the preceding three financial years
* is not a member of the immediate family of an individual who is, or has been during the previous three financial years, employed by the company (or group) in an executive capacity
* is not a professional advisor to the company
* is free from any business or other relationship which could be seen to interfere materially with the individual's capacity to act independently
* does not receive remuneration contingent upon the performance of the company.

2.18.4 ***The board should***

* ensure that there is an appropriate balance of power (and authority) on the board i.e. it should not be dominated by an individual or grouping of individuals.
* consist of individuals of integrity and courage.
* have a suitable diversity of academic qualifications, technical expertise, industry knowledge, experience, nationality, age, race and gender to conduct the business of the board and make it effective.
* have as a minimum, a chief executive officer and a financial director (listed companies must appoint a financial director, this is a JSE requirement). The total number of directors will depend on the nature and complexity of the business and whether it is listed.
* have in place, a structured program to rotate non-executive directors without losing necessary skills. At least one third of the non-executive directors should rotate every year.
* ensure that the independence of any ***independent*** non-executive director who has served for more than 9 consecutive years, is rigorously reviewed.

Element: Board appointment process

Principle 2.19: Directors should be appointed through a formal process.

2.19.1 The procedure for appointing directors to the board should be formal and transparent. The company's Memorandum of Incorporation may include provisions relating to the appointment (and removal of directors) and in the case of a profit company, other than a state owned enterprise, ***must*** provide for the election of at least 50% of the directors (and any alternate directors) by the shareholders.

2.19.2 The board assisted by a nomination committee, should thoroughly investigate the background of the proposed director before appointing or recommending an individual for appointment.

2.19.3 The Companies Act 2008 Sec 69, "Ineligibility and disqualification of persons to be a director" should be carefully adhered to.

2.19.4 It is also important to ensure that a proposed director has not been declared delinquent, and is not on probation in terms of Sec 162 of the Companies Act 2008.

Element: Director development

Principle 2.20: The induction of and ongoing training and development of directors should be conducted through formal processes.

2.20.1 The board should:

* establish a formal induction program to familiarize the new director with the company's business and his responsibilities and fiduciary duties
* ensure new directors with limited experience are mentored
* ensure that formal processes (continuing professional development programmes) are in place to keep directors abreast of important matters such as changes in laws and regulations, accounting standards etc, on an ongoing basis.

Element: Company secretary

Principle 2.21: The board should be assisted by a competent, suitably qualified and experienced company secretary.

2.21.1 The company secretary is a key component of corporate governance. Sec 86 to 89 of the Companies Act 2008 make it mandatory for a public company or state owned enterprise to appoint a company secretary, describe the duties of the company secretary, as well as the resignation or removal of the company secretary.

2.21.2 The board should appoint and remove the company secretary, but the company secretary should have a direct channel of communication to the chairman.

2.21.3 The company secretary should

* have an arms-length relationship with the board
* ***not*** be a director of the company
* assist the nomination committee with the appointment of directors
* assist with the director induction and training programmes
* provide guidance to the board on the duties of the directors and good governance
* ensure board and committee charters are kept up to date
* prepare and circulate board papers
* elicit responses, input, feedback, from board and board committee meetings
* assist in drafting yearly work plans
* ensure preparation and circulation of minutes of board and board committee meetings
* assist with the evaluation of the board, committees and individual directors.

Element: Performance assessment

Principle 2.22: The evaluation of the board, its committees and the individual directors should be performed every year.

2.22.1 For any evaluation to be successfully carried out, the groups or individuals to be evaluated should be fully aware of what they will be evaluated against. Thus they must fully understand their functions and responsibilities. The board should set benchmarks against which performance appraisal will take place.

2.22.2 All directors (executive and non-executive) including the chairman and the CEO as well as the company secretary, should be evaluated.

2.22.3 The chairman may lead the evaluation process or it may be carried out by an independent party. (The evaluation of the chairman should be a process led by an independent non-executive director, and the CEO should be evaluated by the chairman or a board committee appointed for the purpose.)

2.22.4 Evaluations should be carried out, and the results discussed, at least annually and corrective action e.g. additional director training, dismissal etc, taken as necessary. Evaluations should be carried out before nominating directors for reappointment and in deliberating on remuneration.

2.22.5 An overview of the appraisal process, results and action plans, should be disclosed in the integrated report.

Element: Board committees

Principle 2.23: The board should delegate certain functions to well structured committees but without abdicating its own responsibilities.

2.23.1 In terms of Sec 72 of the Companies Act 2008, except where the Memorandum of Incorporation provides otherwise, the board may appoint any number of committees and delegate authority to the committee (but without abdicating the board's ultimate responsibility).

2.23.2 The same section also states that the committee may include persons who are not directors of the company, but that such persons

* must not be ineligible to be or disqualified from being a director ***and*** may not vote on any matter decided by the committee.

2.23.3 In terms of King III, board committees should have formally established terms of reference covering at least

* composition
* objectives, purpose and activities
* delegated authorities (including extent of power) to make decisions and/or recommendations,
* tenure and
* reporting mechanisms.

2.23.4 King III recommends (for larger entities) four standing committees, namely, audit, risk, remuneration and nomination committees. (Note that in terms of Sec 94 of the Companies Act 2008, public companies and state owned enterprises must appoint an audit committee).

*	***Audit committee***	:	chairman should be an independent non-executive director
*	***Remuneration committee***	:	chairman should be an independent non-executive director
		:	all members should be non-executive directors
		:	majority of which should be independent
*	***Nomination committee***	:	chairman should be the chairman of the board
		:	all members should be non-executive directors
		:	majority of which should be independent.
*	***Risk committee***	:	chairman should be a non-executive director
		:	members should include executive and non-executive directors, senior management and independent risk management experts where necessary.

In terms of regulation 43 of the Companies Act, a ***Social and Ethics committee*** must be appointed by

* every state owned company
* every listed public company
* any other company that has in any two of the previous five years, had a public interest score above 500 points.

2.23.5 A director who is not a member of a specific committee may attend meetings of that committee, but may not participate in the proceedings without the consent of the chairman and will ***not*** have a vote.

2.23.6 Terms of reference of committees should be reviewed yearly and disclosed in the integrated report.

Element: Group boards

Principle 2.24: A governance framework should be agreed between the group and its subsidiary boards.

2.24.1 The relationship between holding and subsidiary company boards can present some interesting problems. For example, what is good for the holding company may not necessarily be good for the subsidiary company, but as the holding company has the power to nominate directors to the board of the subsidiary, the real power of the subsidiary's board may rest with the holding company. Conflict of interest may easily arise. Hence:

* the boards of the holding company and the subsidiary should agree on the appropriateness of the implementation and application of policies, processes and procedures of the holding company in the operations of the subsidiary company

* the holding company must recognize the fiduciary duty of the subsidiary company directors to act in the best interests of the subsidiary company even where the director has been nominated to the subsidiary board by the holding company.
* the holding company should consult the chairman of the board of the subsidiary before nominating directors to sit on the subsidiary board to ensure that the director meets the minimum skill, experience, knowledge, integrity etc required by the subsidiary.
* disclosure of the holding company's policies adopted by the subsidiary should be made in the subsidiary's integrated report.

Element: Remuneration of Directors and senior executives

Principle 2.25: Companies should remunerate directors and executives fairly and responsibly.

2.25.1 The remuneration of directors is a very contentious issue, fuelled by frequent "scandals" reported in the press relating to huge bonuses paid to directors (even where the company has performed poorly), the granting of stock options to directors, etc. King III has addressed the issue comprehensively.

2.25.2 Companies should have a remuneration committee which should recommend remuneration policies for all levels in the company but especially senior executives and non-executive directors. The policies should
* create value for the company in the long-term e.g. be attractive enough to retain good staff
* be aligned to the company's strategy, reviewed regularly and linked to performance
* be a mix of fixed and variable pay, in cash, shares and other elements.

2.25.3 Non-executive director's fees (and committee fees) should consist of a retainer and meeting attendance fee, and should be approved by the shareholders in advance. Non-executive directors should ***not*** receive incentive awards e.g. fees based on company performance.

2.25.4 Base pay and bonuses:
* remuneration should reflect the contribution of the executive measured against appropriate and defined criteria
* annual bonuses should relate to performance against annual performance objectives
* performance targets should be reviewed regularly and should be both financial and non-financial
* in measuring performance, multiple performance measures should be used to avoid ***manipulation*** of results or poor business decisions.

2.25.5 Contracts and severance:
* employment contracts with executives should not commit companies to pay out large sums of money where the executive has been dismissed due to poor performance/failure
* early termination of the contract (for other reasons) should not entitle executives to bonuses or share based payments in their severance pay.

2.25.6 Share based and other long-term incentive schemes:
* shareholders should approve in advance, all long-term share based and other incentive schemes
* incentive schemes should contribute to shareholder value and should be reviewed regularly to determine whether they fulfil this objective
* participation in share incentive schemes should be restricted to genuine employees and executive directors and should be subject to appropriate limits for individual participation
* the chairman and non-executive directors should not receive incentive rewards geared to share price or corporate performance
* non-executive directors should not receive share options
* share option awards should not be backdated and should not be exercisable within three years of the date of grant or later than ten years from the date of the grant.

Principle 2.26: Companies should disclose the remuneration of each individual director and prescribed officer.

2.26.1 Sec 30 of the Companies Act 2008 requires full disclosure of directors' remuneration/emoluments in whatever form they may occur. This requirement also applies to persons falling within the Companies

Act definition of a prescribed officer. In terms of Companies Regulation 38 a prescribed officer, is a person who despite not being a director

* exercises or regularly participates to a material degree in the exercise of general executive control over and management of the whole or a significant portion of the business and activities of the company.

2.26.2 The remuneration committee should issue a remuneration report to explain the company's remuneration philosophy and how it has been implemented.

2.26.3 This report should be issued annually as part of the integrated report and should disclose/explain

* the remuneration policies followed, the strategic objectives and the implementation of the policies
* the policy on base pay
* incentive schemes
* share incentive schemes
* material "ex gratia" payments
* the use of benchmarks
* the remuneration of non-executive directors and committee fees.

Principle 2.27: Shareholders should approve the company's remuneration policy.

2.27.1 The company's policy of remuneration should be approved by the shareholders (non-binding advisory vote) in general meeting, but the board is responsible for determining the remuneration of executive directors (in line with the policy).

3. TOPIC 3: AUDIT COMMITTEES

Element: Existence of Audit Committees

Principle 3.1: The board should ensure that the company has an effective and independent audit committee.

3.1.1 The Companies Act 2008, Sec 94 makes it compulsory for a public company and a state owned company to have an audit committee. King III recommends that all other companies establish an audit committee and define its composition, purpose and duties in the ***Memorandum of Incorporation***.

3.1.2 The board should approve the terms of reference of the audit committee.

3.1.3 Meetings

* the audit committee should meet as often as is necessary to fulfil its function but at least ***twice a year***
* the audit committee should meet with internal and external audit (without management being present) at least ***once a year***.

Element: Membership and resources of the audit committee

Principle 3.2: Audit committee members should be suitably skilled and experienced independent non-executive directors

3.2.1 ***All*** members should be independent non-executive directors and there should be at least three members.

3.2.2 The committee should ***collectively*** have sufficient financial knowledge, a good knowledge of financial risks, financial reporting e.g. IFRS and IFRS for SMEs and sustainability/integrated reporting and internal controls.

3.2.3 In terms of Regulation 43 of the Companies Act 2008 at least one third of the members of the audit committee must have academic qualifications, or experience in economics, law, corporate governance, finance, accounting, commerce, industry, public affairs or human resource management.

3.2.4 Where skills are lacking, the board should

* inform the shareholders and recommend that additional directors with the necessary skills be appointed to the committee or
* appoint independent specialists or consultants to the audit committee to provide the necessary skills (consultants should not vote on any matter, this is the responsibility of the committee itself).

Principle 3.3: The audit committee should be chaired by an independent non-executive director

3.3.1 The chairman should be committed to the concept of an audit committee and be able to lead constructive dialogue with management, internal and external auditors and any other external assurance providers.

3.3.2 The chairman of ***the board*** should ***not*** be the chairman of the ***audit committee***. The chairman of the audit committee should be elected by the board.

3.3.3 The chairman of the audit committee, (with the company secretary) should decide on the agenda, frequency and number of meetings, and should attend the AGM.

Element: Responsibilities of the audit committee

Principle 3.4: The audit committee should oversee integrated reporting

3.4.1 Sec 94(7) of the Companies Act 2008, lays down the duties of the audit committee of a public/state owned company. King III aligns with and expands on these duties. Students should study this section of the Act.

3.4.2 The board of a company may delegate its responsibility for reporting and internal control to the audit committee; the audit committee will make recommendations to the board which will, after evaluating the recommendations, approve or reject them.

3.4.3 The audit committee will be responsible for monitoring the integrity and completeness of the company's financial reporting. This will include
* evaluating judgments and reporting decisions e.g. changes in accounting policies, treatment and disclosure of significant or unusual transactions, compliance with IFRS.
* considering whether there are any conditions which may tempt management to "manipulate" the financial statements, e.g. bonuses for management are linked to reported financial performance. (Obviously the audit committee must satisfy themselves that no manipulation has taken place).
* dealing with complaints and queries relating to previously published financial information.
* acting as arbiter/referee between management and the external auditors when there is a disagreement on accounting matters. "Opinion shopping" (management seeks second or third opinions from other auditors when there is a disagreement) should be avoided.
* confirming that other regulatory or enforcement requirements pertaining to the company's financial information is complied with e.g. JSE regulations for listed companies.
* reviewing management's assessment of the company's going concern ability.

3.4.4 The audit committees responsibility extends to the integrity and completeness of all price sensitive financial information including
* the integrated report and financial statements
* interim reports
* preliminary and provisional result announcements
* summarized financial information
* prospectuses

3.4.5 The chairman of the audit committee should be present at the AGM to answer questions on the report of the audit committees activities and matters within the scope of the audit committee's responsibilities. (Shareholders should be encouraged to submit questions prior to the meeting so that suitable responses can be prepared).

Interim results

3.4.6 The board should decide whether

* interim information should be provided every six months or more frequently, e.g. quarterly, and whether
* the interim information should be "audited or reviewed" either by internal or external audit.

3.4.7 Where internal or external auditors perform assurance procedures on interim results, the audit committee should review the results of the engagement.

Summarised financial information

3.4.8 The purpose of summarized annual financial statements is to provide a concise but balanced view of the company's financial information.

3.4.9 The external auditors should be engaged (by the audit committee) to provide an assurance report on summarized financial information, confirming, and indicating in the report, that the information has been appropriately derived from annual financial statements.

3.4.10 Sec 29(3) of the 2008 Companies Act includes a number of requirements which must be adhered to where a company provides summarized financial statements.

Integrated sustainability reporting

3.4.11 The board may delegate the responsibility for the integrated sustainability section of the integrated report to the audit committee (or a sustainability committee).

3.4.12 The audit committee should consider the need to obtain assurance from an external source on the accuracy and completeness of the report. If this is recommended, the audit committee must
* evaluate the independence and quality of the external source
* assist the board in reviewing the sustainability report to ensure it is reliable and has no "conflicts or differences" with the financial results.

Principle 3.5: The audit committee should ensure that a combined assurance model is applied to provide a co-ordinated approach to all assurance activities.

3.5.1 The combined assurance model is the manner in which the company sets itself up to adequately address the significant risks which the company faces, and the audit committee is responsible for ensuring that it adequately addresses the risks.

3.5.2 Combined assurance can be provided by
* internal assurance providers, e.g. internal audit, finance function
* external assurance providers, e.g. external audit, industry regulators
* management.

3.5.3 The relationship between internal and external assurance providers should be monitored by the audit committee.

Element: Internal assurance providers

Principle 3.6: The audit committee should satisfy itself of the expertise, resources and experience of the finance function.

3.6.1 The audit committee should satisfy itself of this by review on an annual basis. The results of the review should be included in the integrated report. Listed companies must have a finance director with suitable experience and expertise.

Principle 3.7: The audit committee should be responsible for overseeing of internal audit.

3.7.1 Internal audit may report directly to the board or to the audit committee. The head of internal audit (chief audit executive) should report directly to the audit committee.

3.7.2 The audit committee should
* be responsible for the appointment/dismissal, performance assessment of the CAE
* approve the audit plan

* ensure that internal audit is independent, and has the necessary resources, standing and authority to discharge its functions
* oversee co-operation between external and internal audit
* evaluate the effectiveness of internal audit by independent quality review
* report to the board on internal audit's assessment of the company's internal controls.

Principle 3.8: The audit committee should be an integral component of the risk management process

3.8.1 The audit committee should have oversight of
* financial reporting risk
* internal financial controls
* fraud risk (as it relates to financial reporting)
* information technology risk (as it relates to financial reporting).

Financial reporting/internal financial controls

3.8.2 Although the board is ultimately responsible for the design, implementation and maintenance of a sound system of internal control, the audit committee should be responsible for overseeing risk management and controls.

3.8.3 The audit committee must understand the environment in which the company operates and the challenges it faces, to be in a position to assess the appropriateness of the company's risk management programme.

3.8.4 The audit committee should report annually to the board on the effectiveness of the company's internal financial controls. The report should include any financial control inadequacies which resulted in actual material financial loss.

3.8.5 To be in a position to make this report, the audit committee should determine the nature and extent of a formal review of the design, implementation and effectiveness of internal controls to be carried out (annually) by management or internal audit. Internal audit would be preferable as they are far more independent.

Fraud risks

3.8.6 The audit committee should consider matters which may result in material misstatements in the financial statements due to fraud.

3.8.7 The audit committee should
* review the arrangements made to enable employees and outside whistle blowers to report concerns about improprieties in matters of financial reporting or compliance with laws and regulations which may affect financial reporting
* ensure that there is a suitable system in place for an independent and balanced investigation into matters reported by whistle blowers.

3.8.8 Sec 159 of the Companies Act 2008 deals with protection of whistle blowers and should be studied in conjunction with this principle.

Information Technology risks

3.8.9 In most companies IT, internal control and risk are intertwined. In addition, IT has inherent risks which will need to be closely addressed.

3.8.10 It is very likely that the audit committee will need expert IT advice to meet their responsibilities with regard to the management of the company's exposure to IT risk.

3.8.11 As a minimum, the audit committee should play an oversight role regarding
* IT risks and controls
* business continuity and data recovery
* data security and privacy

Element*: *External assurance providers

Principle 3.9: The audit committee is responsible for recommending the appointment of the external auditor and overseeing the external audit process.

3.9.1 Sections 90 to 93 of the Companies Act 2008 deals with auditors of public and state owned enterprises and should be studied under this principle. The recommendations of King III align with these sections.

3.9.2 With regard to the external auditors, the audit committee should

* recommend the appointment, re-appointment and removal of the external auditors
* before making this recommendation (annually), assess the audit firm's and the designated auditor's qualifications, expertise and resources, effectiveness (especially when recommending re-appointment) and independence
* approve the terms of the external auditor's engagement and remuneration
* oversee the planning and execution of the annual external audit (the scope of the audit cannot be limited by the audit committee)
* define and implement a policy for the nature, extent and terms under which the external auditor may perform ***non-audit*** services
* review any accounting and auditing concerns arising from the internal or external audit.
* develop a procedure for receiving, considering and resolving reportable irregularities (Sec 45 of the Auditing Profession Act 2005)
* at the end of the annual audit, review the quality and effectiveness of the audit process, by discussion with the external auditor, head of internal audit, finance directors, etc; deviations from the original audit plan should be discussed.

Element: Reporting

Principle 3.10: The audit committee should report to the board and shareholders on how it has discharged its duties.

3.10.1 The report should provide, as a minimum

* a summary of the role of the committee
* whether the audit committee has adopted formal terms of reference, and whether it has complied with its terms of reference
* names and qualifications of all members of the audit committee and the period for which they served
* the number of audit committee meetings held and who attended
* a description of how the audit committee carried out its functions
* a statement as to whether the audit committee is satisfied with the independence of the external auditor
* commentary on the financial statements, accounting practices and financial control of the company
* information on other roles assigned to the audit committee by the board
* recommend the integrated report for approval by the board.

3.10.2 The report by the audit committee to the shareholders should be included in the annual financial statements.

4. TOPIC 4: THE GOVERNANCE OF RISK

Element:The board's responsibility for risk governance

Principle 4.1: The board should be responsible for the governance of risk

4.1.1 The board's responsibility should be expressed in the board charter.

4.1.2 The board should be responsible for the development and approval of a risk management policy and plan which should be

* widely distributed throughout the company
* reviewed once a year and

* its implementation monitored continually.

4.1.3 The board should have the responsibility to ensure that the company has implemented an effective ongoing process to ***identify*** risk, ***measure*** its potential ***outcome*** and ***activate*** what is necessary to ***manage*** the risks (e.g. having management design, implement and monitor controls and procedures).

4.1.4 To be in a position to identify risk, the board must set the company's objectives and strategies and decide on the company's appetite for risk and calculate the company's risk bearing capacity and tolerance limits for key risks.

4.1.5 Risks should not be considered in isolation and their potential for cumulative or multiplicable effects realized.

4.1.6 The board should receive and review, at appropriate intervals, risk management reports based on comprehensive risk assessments.

4.1.7 Essentially business is about taking risks in the expectation of earning a reward. The strategy a company adopts and the business processes it puts in place, are all subject to risk. For example, a company decides that its objective for the next five years is to double its annual turnover. Its strategy to do this will be rather than to purchase locally, to import its products for resale from a cheaper source, and allow more generous credit terms to customers. Simple and superficial analysis immediately reveals some risks.

Risks arising from the chosen strategy may include

* cheaper goods may be inferior in quality
* existing customers may not want to purchase imported goods from certain countries
* a range of foreign exchange regulations must be addressed
* liquidity problems arising from the generous credit terms
* potential breaches of the Credit Act

Risks relating to the business process may include

* inadequate procedures to deal with the expected increase in customers
* inadequate resources to collect payment from debtors in arrears (bad debts)
* inadequate skills to account correctly for foreign currency transactions, forward cover, etc.

Numerous other risks may be identified but this simple example illustrates that risk management, strategy and the operations of the business are inseparable.

Principle 4.2: The board should determine the levels of risk tolerance.

4.2.1 Risk tolerance levels quantify the amount of risk that the company is prepared to accept, relating to an objective, and should be aligned with the company's risk appetite and risk philosophy, e.g. if the company has a low appetite for taking risks, its philosophy will be risk averse and its risk tolerance levels will be low.

4.2.2 Risk tolerance limits should be established for each key risk. In an export business, a key risk may be the rand/dollar exchange rate; the company will need to evaluate the risk of major fluctuation in the rate and the effect this may have on any significant business decisions. If the company has a low risk appetite and risk averse philosophy, it may decide not to enter into a particular business transaction because it can only "tolerate" minor exchange rate fluctuations, and the directors believe that there is a risk of major fluctuations.

4.2.3 As the principle suggests, the indicators, tolerance levels etc, should be laid down and approved by the board.

4.2.4 The risk philosophy is the board's position on the risks in its business environment. Simplistically stated, the company's position will be somewhere on the scale of "risk taking to risk averse".

4.2.5 The board should draft a risk philosophy statement which, inter alia, includes an explanation of the board's position on risk and the factors which shape that position, e.g. regulatory compliance expectations, safety and health demands, sustainability and corporate governance requirements.

4.2.6 Such matters as the company's upper limit beyond which the board would not be willing to put further capital at risk in pursuit of reward, should be determined, e.g. investing R100m in a new venture may expose the rest of the business to unacceptable risk, but investing R50m may be acceptable because the board believes the company could withstand the losses which may arise if the venture fails/ does not come up to expectations.

Principle 4.3: The risk committee or audit committee should assist the board in carrying out its risk responsibilities.

4.3.1 The board may appoint a risk committee specifically to deal with risk management.

4.3.2 If a risk committee is appointed, it should
* be chaired by a non-executive director
* have a minimum of three members (no limit)
* consist of a mix of executive directors and non-executive directors, members of senior management and if necessary, independent risk management experts (who will not have a vote)
* convene at least twice a year
* consist of members who have the qualifications, experience and skills to meet the responsibility of risk management, e.g. IT skills.

4.3.3 The risk committee should
* specifically consider the risks which may affect the sustainability of the company and it may be appropriate to name the committee "the risk and sustainability committee"
* review the risk management maturity of the company
* consider the risk management strategy and policies
* monitor the risk management process.

Element: Management's responsibility for risk management

Principle 4.4: The board should delegate to management the responsibility to design, implement and monitor the risk management plan.

4.4.1 Management is accountable to the board for ***designing, implementing and monitoring*** the process of managing risk and integrating it into the day to day activities of the company, e.g. a second hand car parts dealer needs to have processes (controls and procedures) in place to ensure that the company is not buying and selling parts from stolen cars. A chicken producer needs to have processes in place to minimize the risk of disease.

4.4.2 As can be seen from 4.4.1, risks are very diverse, but it remains the responsibility of management, led by the chief executive officer, to manage those risks.

4.4.3 In larger companies, a chief risk officer (CRO) may be appointed to assist in managing risk. He should have access to the board and interact regularly with it on strategic matters.

4.4.4 The board should review the company's risk management plan at least annually against actual performance and it should be updated where necessary.

4.4.5 In the performance of their day to day activities, all staff are faced by a level of risk. For example, a worker on an assembly line may be exposed to significant health risks, and a credit controller is exposed to the risk of overextending credit. Some risks are clearly far more significant than others, but management should attempt to inculcate, by training and re-enforcement, a culture of risk management. For example, the factory manager, foreman and worker should ensure that the necessary protective clothing is worn and safety procedures are followed to the letter.

Element: Risk assessment

Principle 4.5: The board should ensure that risk assessments are performed on a continual basis.

4.5.1 There are various methods of assessing risk. A systematic, documented, formal risk assessment should be performed at least annually.

4.5.2 Risks should be ranked.

4.5.3 In assessing risk, the board (risk committee) should take into account, inter alia

* ***stakeholder risks:*** e.g. what risks will a proposed expansion of the company, pose for the community in which the expanded business operation will take place? Increase in pollution? Crime? Loss of recreational land?

* ***reputational risks:*** e.g. will the company suffer a loss to its reputation if it fails to support a particular cause or does not take appropriate action against a director convicted of fraud?

* ***compliance risk:*** in relation to legislation which significantly affects the company, e.g. what risks arise for the company if it does not implement the Companies Act requirements adequately? Does an agreement with a competitor in the same business amount to price fixing?

* ***ethics risk:*** e.g. will the introduction of a bonus scheme for sales employees based on sales, increase the risk of unethical selling practices by sales personnel?

* ***sustainability issues:*** e.g. is the risk of loss of employees through HIV/AIDS on the increase?

* ***corporate social investment, employee equity, BEE, skills development and retention:*** e.g. is there a risk that valuable skills will be lost because of poor remuneration packages? Is there a risk that a new promotion strategy will fail to satisfy employee equity requirements?

* ***human and financial capital:*** e.g. is there a risk that a new venture will not generate sufficient cash flow to sustain itself? Will there be sufficient human skills available?

4.5.4 Another framework for risk assessment may be to consider risk in the following categories

* ***strategic risks:*** e.g. the risks associated with adopting or changing company strategy, such as expansion of the manufacturing facility, entering a new market in a foreign country, acquiring another company

* ***operating risks:*** e.g. risks relating to health and safety, and the environment for a chemical manufacturer

* ***financial risks:*** e.g. the effect on cash flows should a company decide to move from a cash sales basis to a credit sales basis, or the risk associated with committing the company to long-term borrowing to finance an expansion

* ***information risks:*** e.g. the risks associated with introducing electronic funds transfer for payment of creditors, or a retail company deciding to introduce on-line trading (note, this could also be classified as a strategic risk)

* ***compliance risks:*** e.g. the risk that a business decision may result in significant breaches of legislation, relating to pollution, the environment, taxation, price fixing, foreign exchange, fraud, etc.

4.5.5 Risk identification should not simply amount to risk committee members giving their opinions, it should be a process which makes use of data analysis, business indicators, market information, portfolio analysis, etc.

Principle 4.6: The board should ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks.

4.6.1 In effect this requires some "crystal ball gazing" by directors! The future is uncertain, and there are any number of unexpected occurrences which can severely affect a company's sustainability. Such occurrences can range from natural disasters, e.g. drought, flooding, to war, to financial collapse and are frequently not predictable.

4.6.2 However, directors are tasked with the duty to consider the sustainability of their companies, and this principle requires that they keep abreast with, political, physical, environmental, economic, social, technological and trade trends. The company's risk assessment process should include sessions for directors at which the "unknown future" is anaylsed, brainstormed and debated possibly on a "what if" basis ……

Element*: *Risk response

Principle 4.7: The board should ensure that management considers and implements appropriate risk responses.

4.7.1 There are models which quantify risk and companies may choose to make use of these. It may be sufficient however, to classify risk as low, medium or high. The important point is that the board and management should develop a clear understanding of the severity of the risks and how they will manage the risk. In determining the severity/significance of the risk, the board (risk committee) may consider such things as

* the probability of risk occurring
* the potential effect of the risk
* how effective a risk response might be
* the threat to solvency, liquidity, going concern.

4.7.2 Once the risks have been identified, the board, risk committee and management, should consider the possible risk response options. Again there are various models to respond to risk, but options will normally include

* ***avoid or terminate*** the risk by not commencing or ceasing the activity which creates the exposure to the risk, e.g. if the company can no longer tolerate the risk of doing business in a foreign country, then close that business down

* ***treat, reduce*** or ***mitigate*** the risk, e.g. exposure to the risk of foreign exchange losses may be treated, reduced or mitigated by taking forward cover

* ***transfer*** the risk to a third party, e.g. if the company considers that the proper maintenance of its computer system, database, etc, is at risk, it may decide to outsource this responsibility. Taking out insurance is a common method of transferring risk

* ***accept*** the risk, e.g. if a transport company's risk assessment reveals that a 100% increase in the cost of diesel to say R25 a litre will seriously jeopardize its going concern ability, but that the risk of this occurring is low, the company may simply decide to accept the risk, rather than perhaps replacing its fleet of vehicles with more fuel efficient vehicles

* ***exploit*** the risk, e.g. where a retailer of expensive clothing anticipates loss of market share due to the economic downturn, it may decide to introduce a range of cheaper clothing to regain its market share

* ***integrate*** a number of options given above.

4.7.3 A risk register should be maintained in which risks and responses to the risk, are recorded.

Element: Risk monitoring

Principle 4.8: The board should ensure continual risk monitoring by management.

4.8.1 The board must set up a process to ensure continual monitoring of the effectiveness of the risk management plan, and the responsibility for risk monitoring should be defined in the risk management plan.

Element: Risk assurance

Principle 4.9: The board should receive assurance regarding the effectiveness of the risk management process

4.9.1 Management should provide assurance to the board that the risk management plan is integrated into the daily activities of the company.

4.9.2 Internal audit should provide the board with a written assessment of the effectiveness of internal control and risk management.

4.9.3 Internal audit should not take on any of the functions or processes of risk management but should assist the board in monitoring risk management in the company. To ensure that internal audit is independent of risk management, the two "departments" should not report to each other and preferably should not report to the same executive.

Element: Risk disclosure

Principle 4.10: The board should ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders .

4.10.1 The board should report on how the company has dealt with risk management in a statement in the integrated report. The board should

* include a statement that the board is responsible for the total process of risk management as well as forming an opinion on its effectiveness
* disclose the system that is in place to evaluate the effectiveness of the process, e.g. independent reviews by internal audit
* confirm that the board maintained a system to monitor changes in the company's risk profile
* make a statement that key risks are being managed and that the board is not aware of any key risk, current, imminent or forecast, that may threaten the sustainability of the company
* disclose any material losses (causes, quantity and effect) and steps which have been taken to prevent a recurrence. (Note: the company is not required to disclose privileged/confidential information).

4.10.2 When the board is not able to make the disclosures required by 4.10.1, it should provide a suitable explanation in the integrated report.

5. TOPIC 5: THE GOVERNANCE OF INFORMATION TECHNOLOGY

Element: The board's responsibility for IT governance

Principle 5.1: The board should be responsible for IT governance

5.1.1 IT policies and an IT charter should be established and implemented.

5.1.2 There should be an ethical IT governance culture which aligns with the company's values e.g. personal information on a company's database should not be sold or made available to other entities unless the individual has given permission.

5.1.3 The board must ensure (through management) that an IT internal control framework is adopted, implemented and independently assessed and reported on.

5.1.4 IT governance is the responsibility of the board, either directly or through the risk committee or some other specifically formed "IT committee"

* board members should play an active role in IT strategy and governance
* the CEO should provide organizational structures to support the implementation of the strategy
* the senior members of the IT division/department must be business orientated (not just technical wizards) and must provide the link between IT and the business
* all executives should become involved in IT steering or similar committees such as an IT strategy committee
* IT matters should be a regular and significant part of the board's agenda

* board members should challenge the IT department's activities with the objective of uncovering issues and problems
* the board should encourage management and IT to work together and should ensure that management understands the effect on the business of IT related risks
* the board should insist that IT performance be measured and reported to the board.

Principle 5.2: The board should ensure that IT is aligned with the performance and sustainability of the company.

5.2.1 It is not difficult to understand why IT is so important to the modern day business and why IT risk is so vital to sustainability. A bank which does not offer the latest computer based services, e.g. electronic fund transfer, full internet banking, ATMs, will lose customers fast. Manufacturing companies may depend upon computers for inventory control, production control and its entire integrated financial reporting system. An insurance company or medical aid may have vast databases of confidential information which must not be compromised in any way.

5.2.2 In addition to the types of risks arising from the few examples given in 5.2.1 above, the costs of installing, running and maintaining a sophisticated computerized system can be considerable; there is therefore a risk that the company could be wasting money if costs are not properly controlled.

5.2.3 All of this requires a process of IT governance and in terms of King III and the IT Governance Institute, IT governance should focus on

* strategic alignment with the business and collaborative solutions, including the focus on sustainability. This simply means that IT and the business are totally interlinked. IT cannot "stand alone" and equally the business operations depend upon IT. It is therefore imperative that IT supports the objectives of the business and that IT and business managers collaborate in solving problems and developing both IT and the business itself, e.g. a company which wishes to introduce trading over the internet cannot hope to be successful without working with its IT department. Similarly an IT department should not be busy developing software which does not meet the needs of the business!
* value delivery, optimizing expenditure and proving the value of IT. The board should not approve IT projects before a thorough cost/benefit analysis has been done which demonstrates the value of the IT project. Once a project is up and running, it should be regularly evaluated to determine whether the expected "return on investment" is being achieved
* risk management, safeguarding IT assets, disaster recovery and continuity of operations
* resource management, optimizing knowledge and IT infrastructure. This means that part of IT governance is ensuring that maximum (optimal) benefit is gained from the use of the IT resources which the company has at its disposal.

Principle 5.3: The board should delegate to management, the responsibility for the implementation of an IT governance framework.

5.3.1 Management should be primarily responsible for the implementation of the IT governance framework (structures, processes, mechanisms).

5.3.2 An IT steering committee may be formed and a chief information officer (CIO) appointed by the CEO, (following appropriate recruitment policies).

5.3.3 The CIO must have access to the board and should interact regularly with it on strategic IT matters.

Principle 5.4: The board should monitor and evaluate significant IT investments and expenditures.

5.4.1 Whilst the investigation/feasibility studies relating to significant IT expenditures will be conducted by the IT steering committee, approval for the expenditure should come from the board.

5.4.2 The board should monitor the return on investment of major IT projects (not always easy to quantify).

5.4.3 Intellectual property contained in the information system (e.g. unique software) should be protected and

5.4.4 Independent assurance on the governance of outsourced IT services should be regularly obtained.

Principles 5.5 and 5.6: IT should form an integral part of the company's risk management and the board should ensure that information assets are managed effectively.

5.5.1 IT management must be able to demonstrate that

* effective disaster recovery plans are in place
* the company is complying with relevant IT laws, rules, codes etc.
* information is secure and protected from unauthorized access, contamination, destruction, etc
* equipment is adequately safeguarded e.g. from theft, damage, etc.

5.5.2 IT security is of paramount importance to the company and therefore should be of paramount importance to the board – poor IT security threatens virtually all aspects of a large business and can threaten sustainability.

5.5.3 Information security has three components

* ***confidentiality***: information should be accessible only to those authorized to have access
* ***integrity***: the accuracy and completeness of information and processing must be safeguarded
* ***availability***: authorized users have access to information when required.

5.5.4 Sound IT security contributes for example, to

* building trust between the company and its business partners, customers and employees. For example, if weaknesses in IT security in an online trading company such as Amazon or Kalahari, result in confidential information about registered customers becoming freely available, customers will simply not be prepared to use the site. Without this trust, new ***business strategies*** attempted by the online trading company, are unlikely to succeed.

* ***sustaining normal business operations***: e.g. if a company's system "crashes" frequently and users cannot get information, the company will lose business. If your bank is frequently "off line" you are eventually going to look for a new bank. If you cannot access an online trading store you are going to search for another store.

* ***avoiding unnecessary costs*** brought about by failure in IT security. This is similar to the previous benefit but perhaps less obvious. For example, breaches in confidentiality could lead to ***litigation*** (very costly) and/or the need to spend money on repairing the reputational damage (marketing campaigns etc) which such litigation often brings.

* ***meeting compliance requirements***. Companies are required to comply with the law in numerous ways. For example, a company must pay VAT. If the process of recording VAT is not secure and the database on which the VAT information is stored is not safeguarded, the amount of VAT indicated as payable may be inaccurate and incomplete or may not be available at all.

These are just a few examples of the importance of IT security but should be sufficient to illustrate the major importance of IT security.

Principle 5.7: A risk committee and the audit committee should assist the board in carrying out its IT responsibilities.

5.7.1 As has been explained, IT can present major risks to the company, thus the risk committee should ensure that these risks are adequately addressed by obtaining appropriate assurance e.g. independent review.

5.7.2 The audit committee should consider IT risk in relation to financial reporting and the going concern ability of the company, e.g. would the collapse of the IT system affect the going concern ability, and if so, has the risk been adequately addressed?

6. TOPIC 6: COMPLIANCE WITH LAWS, RULES, CODES AND STANDARDS

Element: Companies, boards and individual directors

Principle 6.1:The board should ensure that the company complies with applicable laws and considers adherence to non-binding rules, codes and standards.

6.1.1 This means compliance with Acts promulgated in parliament, subordinate legislation and applicable binding industry requirements e.g. JSE listing requirements.

6.1.2 Where there are (legally) non-binding rules or standards which would enhance the company's corporate governance, the company should adhere to them. A company should disclose the applicable non-binding rules and standards to which it adheres on a voluntary basis in its reporting to stakeholders, e.g. there are numerous safety, environmental and industry standards which are recommended but are not "law".

6.1.3 Exceptions, shortcomings and "loop holes" in the law should be handled ethically, and the company should not seek questionable ways of getting around the law; compliance should be an ethical imperative.

6.1.4 The board should monitor the company's compliance with applicable laws, rules etc, and the compliance should be a regular item on the agenda of the board.

6.1.5 The integrated report should disclose details of how the board discharged its compliance responsibilities.

Principle 6.2: The board and each individual director should have a working understanding of the effect of the applicable laws, rules, codes and standards on the company and its business.

6.2.1 The board has a duty to identify the laws, rules, etc, applicable to the company, and part of the induction and ongoing training of directors should be familiarization with applicable laws, rules, etc.

6.2.2 Not all directors need to have an in-depth knowledge of all of the laws etc, applicable to the company. For example, the production director is unlikely to have an in depth knowledge of the Income Tax Act, but collectively the board must have in-depth knowledge and individual directors should have a sound knowledge of laws etc applicable to their portfolios and at least an awareness of other laws etc.

6.2.3 The company secretary has a duty to assist the board/directors in fulfilling their duties with regard to laws, regulations, etc.

Principle 6.3: Compliance risk should form an integral part of the risk management process.

6.3.1 Compliance risk is the risk of damage arising from non-adherence to laws and regulations etc. Damage may be ***financial*** (e.g. losses from penalties, lost contracts), to the company's ***reputation*** (e.g. reports in the media about the company evading taxation), to ***stakeholder relationships*** (e.g. oil refinery breaches health regulations, and resultant pollution affects the local community) or ***sustainability*** e.g. bus company ignores roadworthy requirements placing its operating license in jeopardy.

6.3.2 Like any category of risk, compliance risk should be identified, assessed and responded to through the company's risk management process.

6.3.3 A compliance function may be established. It should

* be independent
* provide assistance to the board and management in complying with laws, regulations etc
* be managed by a qualified and experienced person (compliance officer)
* report on its activities to the board/executive management
* be adequately resourced to fulfil its duties.

Principle 6.4: The board should delegate to management the implementation of an effective compliance framework and processes.

6.4.1 There should be a legal compliance policy, approved by the board and implemented by management.

6.4.2 Compliance with laws, rules, codes and standards should be included in the ***code of conduct*** and management should inform and educate employees in respect of matters pertaining to compliance.

6.4.3 A compliance officer may be appointed, and should be afforded access to the board to interact on compliance matters, e.g. the implementation of a new Act which affects the company and its employees.

7. TOPIC 7: INTERNAL AUDIT

Element: The need for and role of internal audit

Principle 7.1: The board should ensure that there is an effective risk based internal audit.

7.1.1 Change, the complexity of business, organizational dynamics and a more stringent regulatory environment require that (large) companies maintain an effective internal audit function.

7.1.2 Where the board decides not to establish an internal audit function, full reasons for this must be given in the integrated report. An explanation of how the company has obtained adequate assurance as to whether effective governance, risk management and internal controls have been maintained, must also be given.

7.1.3 Internal audit services may be provided by a department within the company itself, or may be outsourced. For example, many large auditing firms provide internal audit services to non-audit clients. Even in this situation, a senior executive of the company (or a director) should be responsible and accountable for the effective functioning of "internal audit".

7.1.4 Internal audit's key responsibility is to the board. It assists the board in discharging its governance responsibilities by

* performing reviews of the company's governance process including ethics
* performing an objective assessment of the adequacy and effectiveness of risk management and internal controls
* systematically analyzing and evaluating business processes and associated controls
* providing a source of information regarding fraud, corruption, unethical behaviour and irregularities.

7.1.5 An internal audit charter should be formally defined, documented and approved by the board (audit committee).

7.1.6 The internal audit function should adhere to the Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing and Code of Ethics.

Element: Internal audit's approach and plan

Principle 7.2: Internal audit should follow a risk-based approach to its plan.

7.2.1 A compliance based approach to internal audit sets out to determine whether or not the company is complying sufficiently with internal controls and other rules and regulations. This is not regarded as sufficiently productive by King III and the recommendation is that internal audit be risk based, i.e. the internal audit function gains a thorough understanding of the risks which the business faces as well as considering whether there are risks which have not been identified, and then conducts tests to determine that an appropriate risk management process is in place and being properly conducted. This does not

mean that there will be no "internal control or other compliance testing". This will still occur as part of the overall function of internal audit.

7.2.2 A risk based audit approach to internal audit (as opposed to a compliance based approach) should be adopted. An audit plan should be developed and discussed with the audit committee. The plan should

* address the full range of risks facing the company, e.g. strategic, operational, financial, ethical, fraud, IT, human and environmental
* identify areas of high priority, greatest threat to the company, risk frequency and potential change
* indicate how assurance will be provided on the risk management process and how the plan reflects the level of maturity of the risk management process. Note: the more mature (developed, effective, well implemented) the risk management process, the more comprehensive the plan can be – it is very difficult to give assurance on an immature risk management process
* have any changes to it, timeously approved/ratified by the audit committee.

Principle 7.3: Internal audit should provide a written assessment of the effectiveness of the company's system of internal control and risk management.

7.3.1 Internal audit should play a major part in the combined assurance framework discussed earlier in this chapter. The combined assurance framework is made up of management, internal assurance providers (mainly internal audit) and external assurance providers (mainly external auditors). It stands to reason that the internal audit department should have the necessary resources and abilities in its staff to involve itself in providing assurance on governance, risk management and internal control. If it does not, it will be unable to report adequately to the board.

Principle 7.4: The audit committee should be responsible for overseeing internal audit.

7.4.1 In a sense, internal audit is the agent of the audit committee, the party which gets out and gathers the information which the audit committee requires to fulfil its responsibilities with regard to risk management.

7.4.2 The internal audit plan should be agreed and approved by the audit committee.

7.4.3 The audit committee should evaluate the performance of internal audit and ensure that it is subjected to an independent quality review.

7.4.4 The audit committee should be responsible for the appointment, performance, assessment (and dismissal) of the chief audit executive.

7.4.5 The chief audit executive should report functionally to the audit committee chairman. This sets up the base for creating a strong working relationship between the two parties and positioning internal audit as a trusted strategic advisor to the audit committee.

7.4.6 The audit committee should ensure that the internal audit department is appropriately resourced and funded.

7.4.7 Internal audit should report at all audit committee meetings.

Element: Internal audit's status in the company

Principle 7.5: Internal audit should be strategically positioned to achieve its objectives.

7.5.1 The key elements in the success of the internal audit function are independence and objectivity. Of course competence is a pre-requisite and if this can be combined with independence and objectivity, internal auditors will command the respect they deserve.

7.5.2 It is important however, that the board ensure that internal audit is provided with the necessary "conditions" to attain and retain the status it requires to fulfil its role. For example

* the board and management should defend and promote the independence of internal audit
* properly qualified and experienced staff with high ethical standards should be appointed to internal audit
* the directors and management should regard internal audit as an integral part of the assurance framework and an indispensable control mechanism in the risk management process
* designating the head of internal audit as a senior member of the company, e.g. Chief Audit Executive (CAE)
* having the CAE report functionally to the audit committee and administratively to the CEO
* giving the CAE direct access to the chairman
* supporting and being seen to support the recommendations of internal audit
* ensuring that internal audit is sufficiently resourced and has an appropriate budget.

7.5.3 As mentioned earlier, if internal audit is to be granted the respect it deserves, its members must be competent, independent and objective as well as ethically sound.

7.5.4 Some of the tasks undertaken by internal auditors are complex and will require a thorough understanding of the latest tools and audit techniques, particularly in the information technology field.

7.5.5 In addition, internal auditors require appropriate business skills to enable them to understand the business and organizational dynamics of the company.

7.5.6 The CAE will set the tone of the internal audit function and should have at least the following attributes
* strong leadership
* command respect for his competence and ethical standards
* be a strong communicator, facilitator, influencer, networker and innovator
* have a practical approach
* be able to think strategically and have strong business analysis skills.

8. TOPIC 8: GOVERNING STAKEHOLDER RELATIONSHIPS

Element: Stakeholders and the company

Principle 8.1: The board should appreciate that stakeholders' perceptions affect a company's reputation.

8.1.1 The gap between stakeholder perceptions and the performance of the company should be managed to enhance or protect the company's reputation and should be a regular agenda item.

8.1.2 The board should identify its stakeholder groupings (see 8.2.9) and adapt its relationship with each grouping to best deal with negative (and positive) perceptions.

Principle 8.2: The company should proactively manage the relationship with its stakeholders.

8.2.1 Stakeholders in a company go well beyond the obvious e.g. shareholders and employees. Stakeholders are any group which can affect, or be affected by the company such as shareholders, employees, creditors, lenders, suppliers, customers, regulators, the media, analysts, the community in which the company may operate etc. A company does not operate in a vacuum, it is a widely interactive entity.

8.2.2 The board should therefore identify stakeholders relevant to the company's sustainability to ensure that they are accommodated in the reporting process.

8.2.3 The effect that a particular stakeholder group may have on the company may be direct or indirect. For example, it is reasonably obvious that a long-term strike will directly affect operations of the company (and hence sustainability); it is less obvious that there may be an indirect negative affect on the reputation of the company, which may also have an affect on its sustainability.

8.2.4 The stakeholder inclusive corporate governance approach is aimed at managing the relationship between a company and its stakeholders. Such an approach will have a good chance of enhancing stakeholder confidence, relieving tensions and pressures, enhancing/restoring the company's reputation and aligning differing expectations, ideas and opinions on issues.

8.2.5 Managing stakeholder relations should be proactive. It is mainly about communication (and constructive engagement) both formal (AGM, meetings with regulators) but can also be through informal processes such as social functions, websites, media, "feed-back" sessions to the community, employees, etc.

8.2.6 Essentially this principle requires that companies promote positive, constructive stakeholder activism. Obviously the board needs to act in the best interests of the company and must guard against activism which seeks to damage the company's operations or reputation. For example, a disgruntled journalist may seek to damage the company by constant negative reporting. The board will need to react carefully to this to ensure that the journalist's cause is not strengthened by, for example, aggressive personal attacks in the media on the journalist.

8.2.7 The company and its stakeholders should collaborate in attempting to work in the best interests of both "parties". A collective effort on good governance, benefits the company and its stakeholders.

8.2.8 The collective effort in effect should be aimed at sustaining all the stakeholders. For example, the company needs to foster good relations with its employees as this will result in better performance. At the same time, employees should work hard and be loyal to their employer. This does not mean they should accept unfair labour practices etc, but should be mature in their approach to dealing with it. The company needs good employees and the employees need the company, and their actions should engender mutual respect.

8.2.9 The major stakeholders and the underlying factors on which the relationships with these stakeholders should be built, are as follows:

Suppliers:

* It is in the interest of the company to have stable suppliers who supply products or services of the necessary quality at an acceptable price, when required.
* This is especially important for suppliers of strategic products or services e.g. a sugar milling company is entirely reliant on its transport supplier to deliver sugar cane to the mill if it has outsourced this function. Equally, the transport company will have invested heavily in capital expenditure and needs the contract with the sugar milling company to remain in business.
* A mutually beneficial relationship contributes to the sustainability of both companies.

Creditors:

* These are stakeholders to whom the company owes money; the company should be mindful of the fact that creditors, if not paid, have the power to have business rescue processes imposed on the company and in more serious situations, have the company liquidated.
* Creditors should be managed accordingly, paid on time at the correct amount. Payment terms should be fair to both parties.
* Creditors are usually suppliers either of goods, services or finance and a mutually beneficial relationship should be developed. For example a large supermarket chain should not push its payment terms for smaller suppliers to 120 days when they should be 60 days, just because they have the power to do so, knowing that the small supplier depends on the large supermarket chain.

Employees:

* Employees are arguably the most important asset the business has, and are very often the difference between successful and unsuccessful businesses.
* Companies should engage their employees in improving the business ensuring that employees at all levels benefit from the improvement, e.g. incentive schemes, bonuses, etc.
* The company should also ensure that employees have a chance to develop their potential and capabilities by providing training, a healthy and safe working environment and the opportunity for employees to advance in the company.
* Proper leadership which includes strong communication with employees is essential. Failing to manage employees properly may result in low morale, poor productivity and work quality, strikes, "go-slows" or even sabotage. Good quality staff may be difficult to recruit and keep in the business.

Government:

* Although perhaps not an obvious stakeholder, government is very much a stakeholder.
* A company should abide by the laws of the land and in particular pay taxes due by it in whatever form the tax may be, e.g. normal tax, VAT, import duties, etc. Where a company is required to comply with withholding tax provisions, it should do so.
* ***All*** employees who deal with government (including local and provincial) and civil servants at any level, should
  - act in a manner which promotes mutual respect and co-operation
  - ***not*** engage in any form of corruption with government at large, or any civil servant.
* Companies should not give "major gifts" to politicians or other government officials and should consider carefully whether it is appropriate to make financial contributions to political parties or similar groupings.

External Auditors:

* The company should not view the external audit function as an unnecessary cost or as a threat or imposition to management.
* There is little doubt that a properly conducted external audit is of real value to a company. It adds significant credibility to the financial statements and is an integral ***independent*** element of the combined assurance model. The audit may also be an early warning system of pending problems.
* Essentially external audit is appointed by and accountable to the shareholders, but in reality indirectly benefits all stakeholders.
* External audit works mainly with management and the audit committee, and company policy should promote co-operation between the parties, a free flow of information and an appreciation of the independence requirements of external audit.

Consumers/ customers:

* The saying "the customer is king" has a great deal of truth to it. Without customers the company is not sustainable. A customer is anyone who uses the company's products and services and can range from individuals to the government, to large corporations.
* For customers to respect a company, the company
  - should market responsibility e.g. not glorify products which can be harmful to health such as cigarettes, alcohol, certain food products
  - should communicate product information e.g. content breakdown on foodstuffs, safety precautions for electrical products
  - should not sell products which, for example, are harmful to the environment, customers' health or which have been manufactured in labour "sweat shops" or under other adverse situations.

Industry:

* A company's sustainability is dependent on other entities within its sphere of operations. A company should therefore acknowledge its responsibility to its industry as a whole.
* To achieve this, a company should participate in or facilitate forums to address industry risks and opportunities. (Most industries have such bodies).
* Companies should not engage in anti-competitive practices/price fixing. Firstly, it is against the law and secondly, is counterproductive to the general economy and public, e.g. price fixing by fertilizer companies will result in substantial fines for the companies involved, huge increases in fertilizer costs and increases in food prices.

Local communities:

* Every company operates in a community to some degree or another. A community may be totally dependent on the company and in fact may have been created by the company, e.g. remote mine or forestry operation.
* Looking after its community, amounts to a company being a good corporate citizen, and should be geared to enhancing the lives of local communities by health programmes, schooling, sporting opportunities, etc.

Media:

* The media provides a window into the company for many stakeholders. Media companies employ financial journalists, many of whom have significant knowledge about the company and a platform to air their views.

* It is important therefore that a mutual relationship of trust be developed between the company and the media. If this is to be achieved, the company should be

- open to communication with the media
- accurate and truthful with the information it provides to the media
- professional in its approach e.g. not aggressive or condescending
- objective when assessing reporting by the media e.g. not overreacting when a journalist criticizes the company.

* Likewise the reporting journalist should
  - be knowledgeable and experienced
  - report accurately and fairly without sensationalism
* As with all forms of communication, the company is not expected to compromise its confidentiality standards or its competitive edge.

Regulators:

* King III defines a regulator as a body which seeks compliance either on a mandatory or voluntary basis, with a set of rules or regulations or a code. For example, the JSE "regulates" listed companies; most industries have bodies which regulate practices within their specific industries.
* The relationship between a company and its regulators is similar to that between a company and government. The company should comply with regulations, pay any fees due, deal with the regulators employees with professionalism and not engage in dubious practices to circumvent a regulation, e.g. attempt to bribe an official who is carrying out a regulatory health inspection.

Potential investors:

* Potential investors, i.e. those who may be seeking to invest as opposed to existing shareholders, will expect high standards of corporate governance, board integrity and confidence in the sustainability of the business of the company.

* To enable potential investors to evaluate these aspects, clear and transparent disclosure should be available to them, e.g. on a website, contained in media releases, etc. Frequently large companies will meet with financial journalists and potential institutional investors (e.g. pension funds) to communicate this information.

Principle 8.3: The board should strive to achieve the correct balance between its various stakeholder groupings, in the best interests of the company.

8.3.1 It is often perceived that the most important stakeholders in the company are the shareholders, and that the board's major responsibility is to this body, e.g. profits must be made, share prices maintained, etc.

8.3.2 However, the interests of different stakeholders may well clash and it is in these situations that the board should attempt to satisfy the needs of all shareholders. This provides a better chance of sustaining the company. For example, a fertilizer company may want to expand its operations. It has a choice of two sites. Transport and construction costs on ***site A*** will be much cheaper and the company will earn a far greater return on investment if it expands to ***site A***. However, expansion on ***site A*** will also negatively affect the local fruit farming community. ***Site B*** will be expensive for the company to develop and return on investment will be lower, but there will be no negative affect on local business, and job opportunities will be created for the local community. Does the board go for ***site A*** or ***site B***? A simple management accounting exercise may well prove that ***site A*** is the correct choice financially (and for shareholders) but the task of the board is to decide what will be best for all stakeholders and the long-term sustainability of the company. This would suggest that ***site B*** is preferable.

Principle 8.4: Companies should ensure the equitable treatment of shareholders.

8.4.1 Not all shareholders are equal! There are different classes of share with different rights. There are majority shareholders and minority shareholders, and controlling shareholders and non-controlling shareholders.

8.4.2 This principle requires that despite these differences, shareholders be treated fairly. For example, minority shareholders should be protected against the abusive actions of majority or controlling shareholders.

8.4.3 The Companies Act 2008, Chapter 7 provides remedies for aggrieved parties (including shareholders), but whenever possible the board should set up processes which allow for constructive engagement to minimize the costs and time taken up by the more formal remedies, e.g. the company could set up a shareholder liaison forum.

Principle 8.5: Transparent and effective communication with stakeholders is important for building and maintaining their trust and confidence.

8.5.1 If stakeholders do not receive information which is sufficient, relevant, accurate, honest and timeous, the communication of the information is unlikely to contribute to meaningful stakeholder involvement in the corporate governance process.

8.5.2 Information should be provided on both the negative and positive aspects of the company's performance, and particular attention should be paid to the wording of negative situations. The negatives should not be hidden behind complex/technical language designed to confuse stakeholders.

8.5.3 Whilst transparency is very important, what is disclosed must be considered in the light of
* legal requirements including those applicable to access of information ***and***
* the maintenance of the company's competitive advantage.

8.5.4 The board should also consider the suitability of the method used to communicate, e.g. an information website may be a cheap and effective method but stakeholders, such as a local labour community, may not have easy access to computers!

Element: Dispute resolution

Principle 8.6: The board should ensure disputes are resolved as effectively, efficiently and expediously as possible.

8.6.1 In terms of their duty of care, directors are required to resolve disputes effectively, efficiently and as quickly as possible.

8.6.2 It is the board's duty to set up mechanisms/processes to resolve disputes, e.g. where a dispute arises with an employee, there must be a laid down procedure for that employee and the company to follow. Where there is a dispute (e.g. unlawful strike) with a labour union, there is an established legal procedure which must be followed; the company must have processes in place to adhere to the legal procedure.

8.6.3 Disputes can be internal (e.g. with an employee or shareholder) or external (e.g. with a supplier, customer, local community), and are simply a part of "doing business". Obviously disputes can be taken to court but this is generally costly and time consuming.

8.6.4 ***Alternative dispute resolution*** (ADR) is now a widely accepted practice which involves the parties to the dispute taking the matter to arbitration, adjudication or mediation. This essentially amounts to a party independent of the disputing parties, hearing both sides of the dispute and "presenting a finding or solution"
Note: The Companies Act 2008 recognises the principle of alternative dispute resolution for disputes arising out of Companies Act provisions. See Sec 156 and related sections.

8.6.5 The directors should select a dispute resolution method that best serves the interests of the company. For example, going to court, arbitration or adjudication results in a judgment, whereas mediation or conciliation allows the dispute parties and an impartial and neutral third party to work together to negotiate a resolution to their dispute. (A settlement agreement rather than a handed down judgment.)

8.6.6 In deciding on which dispute resolution method to follow, the board should consider at least the following factors:

* ***time available to resolve the dispute*** – court proceedings can continue for years with postponements, appeals, etc. ADR can be concluded more promptly. It is usually in the interests of the disputing parties to resolve the matter promptly.

* ***principle and precedent*** – where the company wants a binding decision on an important matter of principle, which will result in a precedent for any future disputes, a court action is likely to be more suitable.

* ***business relationships*** – ADR, especially mediation/conciliation is normally far more "friendly" than court proceedings. It is important to maintain good business relationships (sustainability) and mediation/conciliation is more likely to contribute to the continuation of good business relationships.

* ***expert recommendations*** – where the parties do not wish to go to court, but do not have the necessary expertise to devise a solution, an expert may be required to facilitate a solution. (This would be conciliation).

* ***confidentiality*** – where confidentiality for the dispute parties is very important, ADR may be more suitable as dispute resolution proceedings may be conducted in confidence.

* ***rights and interests*** – as indicated in 8.6.5, court proceedings, arbitration and adjudication results in the decision maker (e.g. judge) imposing a resolution of dispute on the parties based on the principles and rights applicable to the dispute. This will usually result in a narrow range of outcomes. Mediation and conciliation allow the parties a level of flexibility, innovation and creativity in fashioning a mutually beneficial solution. For example, a court decision in respect of a breach of contract between a company and its major supplier, might impose a significant financial penalty on the supplier which would be detrimental to the supplier and the business relationship between the two parties. Mediation or conciliation on the same dispute could result in no financial penalty but an agreement by the supplier to change its pricing policy and for the contract between the company and supplier, to be redrafted.

* ***empowerment of participants*** – if mediation or conciliation is to be promptly and successfully concluded, the personnel involved must be given the necessary powers to act.

8.6.7 The success of ADR is largely dependent on the willingness of the parties to resolve the dispute. Obviously presentation skills, a thorough knowledge of the subject matter of the dispute and a professional approach are pre-requisites. Those who fall short of the "will and capacity" to resolve the dispute, should be excluded. Thus the board should select the appropriate individuals to represent the company in ADR.

8.6.8 As discussed earlier, it is becoming more and more common for companies to include an "alternative dispute resolution" clause in business contracts. This clause essentially commits both parties to ADR in the event of a dispute. It is interesting to note that the ADR clause recommended by the Institute of Directors and the Arbitration Foundation of South Africa, includes the phrase "the parties (to the dispute) shall seek an amicable resolution to such dispute…" This will depend largely on the attitude and will of the participants.

9. TOPIC 9: INTEGRATED REPORTING AND DISCLOSURE

Element: Transparency and accountability

Principle 9.1: The board should ensure the integrity of the company's integrated report.

9.1.1 For the company to be transparent and accountable to all of its stakeholders, effective communication is essential. This means that reporting by the company should be

* proactive and
* relevant and transparent
* cover all material matters affecting the company
* integrated across all areas of performance and

* include reporting on ***economic, social*** and ***environmental issues*** (triple bottom line).

9.1.2 There should be controls in place e.g. verification and review of data, to ensure the integrity of the integrated report.

9.1.3 The audit committee should evaluate sustainability disclosures.

9.1.4 Transparency in reporting sustainability information is critical if the trust and confidence of the stakeholders in the company is to be maintained.

9.1.5 Transparency requires that both the positive and negative be reported on, and where negative matters are reported, the company's plans to reduce the effect of this should be disclosed. For example, a fishing company's sustainability may be threatened by the withdrawal of the company's fishing licenses by local government. This should be disclosed as well as the company's response, e.g. lobbying government, moving the operations elsewhere, or merging with other fishing companies.

9.1.6 Sustainability reporting should address the needs and expectations of both internal stakeholders (e.g. employees) and external stakeholders (e.g. the local community, where this is applicable).

9.1.7 Although transparency is a key requirement for sustainability reporting, confidential information should not be disclosed. Obviously non-stakeholders will have access to what is reported and should not be provided with an easy opportunity of acting in a manner which may harm the company, possibly even affect its sustainability.

9.1.8 The integrated report should be prepared every year.

Principle 9.2: Sustainability reporting and disclosure should be integrated with the company's financial reporting.

9.2.1 The Global Reporting Initiative guidelines have become the accepted international standard on sustainability reporting. This provides parameters on "what and how" information should be reported. To be able to produce the information, these guidelines should be built into the company's reporting process. For example, if a company reports on its HIV/AIDS prevention activities, the reporting system should be able to provide the information necessary to make the report meaningful for stakeholders.

9.2.2 As a minimum, the integrated report should include commentary on the financial results, going concern, and how profits have been made (or losses suffered).

9.2.3 Reporting to stakeholders is not just a matter of compiling the annual report and making it available to stakeholders; this would be a minimum requirement.

9.2.4 Each company will have different stakeholders and stakeholders will have different information needs, so each company should decide for itself on the frequency and method of reporting to its stakeholders.

9.2.5 The method of reporting may include meetings, e.g. feedback sessions on pollution to the community in which a company has its manufacturing operations, written reports, e.g. the annual report, or posting information on the company's website. There are a number of standards to assist companies in deciding on what is most suitable for their circumstances, e.g. the Global Reporting Initiative.

Principle 9.3: Sustainability reporting and disclosure should be independently assured.

9.3.1 General oversight for sustainability reporting should be delegated to the audit committee.

9.3.2 The audit committee should review the integrated report to ensure that information is reliable, relevant, understandable and complete (all material matters dealt with).

9.3.3 The audit committee may seek the provision of independent assurance.

CHAPTER 5

GENERAL PRINCIPLES OF AUDITING

CONTENTS

		Page
INTERNAL CONTROL		
1.	Introduction	5/3
2.	Limitations of internal control	5/4
3.	Definition of internal control	5/5
4.	Components of internal control	5/5
5.	Internal control in smaller entities	5/18
6.	The external auditor's interest in internal control	5/19
AUDIT EVIDENCE		
1.	Introduction	5/20
2.	Sufficient appropriate audit evidence	5/20
3.	Financial statement assertions	5/23
THE AUDITOR'S TOOLBOX		
1.	Introduction	5/25
2.	Why perform tests of controls?	5/27
3.	Why perform substantive procedures?	5/28
4.	Vouching and verifying	5/28

AUDIT SAMPLING

1.	Principles of sampling	5/29
2.	Definitions	5/29
3.	Tests of controls and sampling	5/30
4.	Substantive procedures and sampling	5/30
5.	Statistical versus non-statistical approaches	5/30
6.	Steps in the sampling exercise	5/31
7.	Conclusion	5/33

INTERNAL CONTROL

1. INTRODUCTION

1.1 Internal control and risk

Before discussing internal control in the context of an audit, we need to obtain an understanding of what internal control is all about. Why do we need internal controls? What do they achieve? What is their purpose?

We are all exposed to "internal controls" every day of our lives sometimes without even being aware of it. For example, if we want to enter the university library, we must produce a student or staff card, if we want to draw money from an ATM we must enter our PIN number and if we catch a train or bus, or buy something at a shop, we are given a ticket or receipt. All of these procedures are designed to address and limit potential ***risks***. The university restricts access to its library as it believes that allowing anybody into the library is a security risk. Books may be damaged or stolen or may be lost as there will be no efficient means of controlling the issue and return of books. In effect, the university would be failing to protect one of its important assets, namely its library. The risk which the bank is addressing is similar – by requiring a customer to enter a PIN number, they are protecting the customer (and of course themselves) against the risk of theft. What about the tickets and receipts? The risks that they address may not be that obvious. Firstly, a ticket or receipt is a "proof of purchase" which provides the customer with a means of protecting himself from the risk of being wrongly accused of taking a free ride or shoplifting. Secondly, the issuing of a ticket or receipt will be one of a number of controls which the business selling the ticket or issuing the receipt, implements to address the risk that its employee makes a sale for which there is no record and steals the "proceeds".

Of course this is a superficial look at internal control but it illustrates the very fundamental concept that the purpose of internal controls is to address the risk of something undesirable, unintended or illegal, from occurring.

1.2 Internal control from a business perspective

Even though as individuals, we are surrounded by internal control, as auditors, we need to understand internal controls from a business perspective. In a business, management (in its various forms) is responsible for running all aspects of the entity. The objectives of the business will be set, the risks relating to achieving those objectives will be identified and suitable books, records and documents, and policies and procedures will be in place to address those risks. This will include addressing the risks associated with such matters as:

* safeguarding the assets of the company, e.g. inventory, from theft or damage
* preventing fraud
* complying with the laws and regulations applicable to the entity
* producing reliable financial information necessary to run the business and satisfy the financial reporting requirements, e.g. producing the annual financial statements
* operating the business efficiently and effectively.

Internal control is the responsibility of everyone in the business, those charged with governance of the company (e.g. the board of directors), management at all levels as well as ordinary employees;

* the board will have overall responsibility and accountability, especially for identifying the risks of the business which need to be addressed
* management (at different levels) will also be involved in the process of identifying risk and will be primarily responsible for designing and implementing (putting in place) the necessary books, records, documents, policies and procedures to address the risks. Management will also be responsible for maintaining the internal control process i.e. ensuring that policies and procedures are carried out properly and timeously and that they remain effective
* most of the time, it is the ordinary employees who are responsible for executing the internal control procedures, e.g. signing a document, issuing a receipt, reconciling an account, and the success of the control procedure will depend on them. In addition, ordinary employees often have a far better understanding of their functions and may be well placed to participate in the risk assessment process. Many companies have "suggestion box" schemes which reward

employees for coming up with better ways of doing things, including improvements to internal control.

You will probably have realized already that internal controls are not one hundred percent foolproof and that there is no single control which neatly addresses each identified risk. Internal control policies and procedures are fallible and work best in combinations. If we consider the examples given under 1.1, providing you with a student identity card to address a security risk is of little value if the issue of the ID cards is not strictly controlled, or if your card is not used in the process of entering the library. Either a security guard must compare you to the photograph on your identity card or you should have to scan your card through an access turnstile. Again, these controls on their own may also be ineffective – the security guard may not do his job properly or you might give your ID card to a non-student friend! With regard to the PIN number, someone may obtain your PIN illegally or you may give it to somebody. Even if the cashier gives you a receipt for that purchase, it will be of no use unless a record of the sale, which the cashier cannot alter, is kept and an individual, other than the cashier, reconciles the actual cash on hand with the record of sales for the day. Of course management could go piling one internal control procedure on top of another, for example, employ two security guards checking every student's ID card at the library. However, this would be expensive and probably counter productive to the smooth operation of the library and would still not be foolproof!

1.3 What have we learnt about internal control?

* ***Internal control is a process***. It is a combination of systems, policies and procedures designed, implemented and maintained to address the risks of running a business.

* ***Internal control is effected by people.*** It does not consist solely of policy and procedure manuals, ledgers and documents, computers and machines; it involves people at every level of the organization carrying out an assortment of tasks.

* ***Internal control is not the sole responsibility of management***. There is a shared responsibility for the internal control process; the directors, management and ordinary employees are all, in their own ways, responsible.

* ***Internal control is not static.*** It is essentially a response to the risks of operating a business; risks change, responses must change.

* ***Internal control is not foolproof.*** It provides only reasonable assurance that the risks that threaten the objectives of the business will be addressed to the extent that the objectives will be achieved (see limitations of internal control below).

* ***Internal control is not a case of a single control addressing a single risk.*** Internal control policies and procedures must work in conjunction with each other and with the books, records and documents used. The control over a risk is best achieved by combinations of actions, policies and procedures.

2. LIMITATIONS OF INTERNAL CONTROL

As discussed earlier, the control policies and procedures which are put in place at a business, do not provide absolute assurance that the risks that threaten the objectives of the business will be adequately responded to. Besides the fact that some risks may not be identified in the first place, management may ***design*** an internal control system which theoretically, will achieve its objectives but because of the inherent limitations of internal control discussed below, will not do so in its practical application.

2.1 Management's usual requirement that the cost of internal control does not exceed the expected benefit to be derived (cost/benefit)

Example: To safeguard its inventory of shoes, a footwear manufacturing company could store the shoes in an underground vault, have armed guards patrolling with dogs, and demand security clearance from anyone entering the property! The inventory would definitely be safeguarded but at an exorbitant and unnecessary cost. Remember though, that this extent of control will be necessary for a company which carries a large inventory of diamonds or precious metals.

2.2 The tendency for internal controls to be directed at routine transactions rather than non-routine transactions

Example: Internal controls to record the sale of the company's normal trading inventory will have been designed around the receipt of a customer order, a picking slip (a document used to select goods from stores to fill the order) and a delivery note. The documents will result in an invoice being made out. Occasionally a company may sell a non-trading item, such as old company furniture or an old vehicle and in this situation it is unlikely that there will be a customer order, a picking slip (the item being sold is not picked from stores) or a delivery note. Hence there is a risk that the sale will not be raised (entered in the records), as it is a non-routine transaction.

2.3 The potential for human error due to carelessness, distraction, mistakes of judgement and the misunderstanding of instructions

Example: A recently appointed sales clerk calculates discounts on a sale after VAT has been charged, either because he does not understand what he is supposed to do or he is simply careless.

2.4 The possibility of circumvention of internal controls through the collusion of a member of management, or an employee, with parties outside or inside the company

Example: The warehouse supervisor in charge of receiving goods (from suppliers) at a supermarket is required to check the quantity and description of goods being delivered against the supplier's delivery note and sign the delivery note to acknowledge the receipt of say, 400 cartons of milk powder. The warehouse supervisor colludes (makes a fraudulent secret agreement) with the supplier's delivery personnel, e.g. the driver, to sign for 400 cartons but only to take 350, cartons. The driver keeps 50 cartons in his truck, sells them somewhere else and splits the money with the warehouse supervisor. According to the paperwork, the company has received 400 cartons and will pay the supplier the amount due for 400 cartons, although it has only received 350 cartons.

2.5 The possibility that a person responsible for exercising an internal control could abuse that responsibility, for example, a member of management overriding an internal control

Example: A clothing retailer may have a policy which states that a debtor (customer) may not make a purchase if his account is overdue. The shop manager may override this control without authority because the customer is a friend or family member.

2.6 The possibility that control procedures may become inadequate due to changes in conditions and, therefore, compliance with procedures may deteriorate

Example: A company may experience a steady but definite increase in sales to the extent that the only way that its salesmen can keep up with the demand from customers, is by ignoring certain controls. They may stop checking the customer's credit limits before the sale is made or confirming that the customer's account is up to date. Controls have remained static, but risks have changed.

The preceding pages are designed to give you a general understanding of internal control. The following pages will look at internal control in a more formal context.

3. DEFINITION OF INTERNAL CONTROL (ISA 315(revised) para. 4)

Internal control can be defined as the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to:

* the reliability of the entity's financial reporting
* the effectiveness and efficiency of its operations and
* its compliance with applicable laws and regulations.

4. COMPONENTS OF INTERNAL CONTROL (ISA 315 (revised) para. A76)

The literature on internal control provides a useful framework for understanding internal control. This framework suggests that internal control consists of five components and on page 5/6 you will find a chart of the important points relating to each of the five components. The points raised in the chart, are supported by a narrative discussion about the component and the point itself. Unfortunately these narrative discussions can be quite long and "wordy" and it is easy to lose sight of where you are in the overall process of internal control; the summary chart is there to re-orientate you with a quick glance.

The components of internal control – an overview

Control environment (4.1) Refer ISA 315 (revised) para. 14 and para. A76 and A77	Risk assessment process (4.2) Refer ISA 315 (revised) para. 15 and para. A87	Information System (4.3) Refer ISA 315 (revised) para. 18 and para. A89	Control Activities (4.4) Refer ISA 315 (revised) para. 20 and para. A96	Monitoring of controls (4.5) Refer ISA 315 (revised) para. 22 and para. A106
* integrity and ethical values * commitment to competence * participation of those charged with governance * management's philosophy and operating style * organizational structure * assigning authority and responsibility * human resource policies and practices	* define the objectives of the entity, its departments and functions * identify and assess risks • operational • financial reporting • compliance * respond to risk • information system • control activities	* valid, accurate and complete * procedures and records to deal with transactions • initiating • recording • processing • correcting • posting (to ledgers) * related accounting records • documents used • document design * capturing events and conditions other than transactions * journal entries	* actions, procedures supported by policies • approval, authorization • segregation of duties • isolation of responsibility • access/custody (security) • comparison and reconciliation • performance reviews * preventive, detective * general and application	* assessment over time * are objectives being met? * assessment at all levels • directors • management • department heads * independent assessment • internal audit • external bodies • customers * remedial action

4.1 The control environment.

This is the control consciousness of the entity. It includes the governance and management functions and the attitudes, awareness and actions of those charged with governance and management concerning the entity's internal control and its importance. The control environment sets the tone of the entity and creates the atmosphere in which employees go about their duties. An effective control environment is one in which employees are competent, understand their duties, the limits of their authority, and are committed to "doing things the right way". Such employees will commit to the entity's policies and procedures in a constructive manner and subscribe to sound ethical standards and appropriate standards of behaviour. The control environment is about technical competence and ethical commitment.

4.1.1 Communication and enforcement of integrity and ethical values.

If employees at all levels (directors, management and lower level employees) do not act with integrity (straightforward and honest) and with a strong sense of ethics, internal controls will not be effective. A corrupt individual will find ways of stealing from the organization through devious and dishonest ways. Theft and fraud are clearly risks which all organizations face and the internal control process attempts to address this risk. Having individuals in the process whose ethics and behavioural standards are dubious, will weaken the system. Whilst the vast majority of people understand the fundamental requirements of integrity and ethical behaviour, they will still need guidance on situations which arise in the business environment. For example, we all know that stealing is wrong but what actually constitutes stealing in a business context? Is making that private phone call at the company's expense, stealing? What about taking "sick leave" when you aren't sick? Sneaking home early? Using the entity's vehicle as a private taxi at the weekends? Taking the odd item because "the company won't miss it"? Accepting that gift from a supplier? The list is endless and the point is, employees need guidance and direction. Thus the entity's policies on integrity and ethical values should be communicated to all employees by means of policy statements, workshops and codes of conduct. Management should also attempt to eliminate or reduce incentives or temptations which might prompt or encourage employees to engage in dishonest, illegal or unethical behaviour. On a general level, this may be achieved by providing fair remuneration and pleasant working conditions. At a specific level it is achieved by implementing sound control activities. Finally, there must be a disciplinary mechanism which deals with transgressions of the entity's ethical and behavioural standards. The reality is that the control environment is influenced by the extent to which individuals know that they will be held accountable for their ethical behaviour.

4.1.2 Commitment to competence.

A competent employee is one who has the necessary knowledge and skills to do his job. In a business where everyone knows what to do and how to do it, the control environment will be significantly improved. For individuals to function beyond their capabilities can be stressful and discouraging, which in turn may lead to behavioural problems. This can be addressed by management

* defining jobs carefully and identifying competency requirements for the job
* filling the position on merit
* providing ongoing training and the tools to do the job
* rewarding excellent performance.

4.1.3 Participation by those charged with governance.

The entity's control consciousness is strongly influenced by those charged with governance, primarily the board of directors. If the directors, by their actions, do not demonstrate a commitment to ethical behaviour as well as the internal control process, the control environment will decline. Management will generally follow the example of the directors and lower level employees will follow the example of management! Laws and regulations such as the Companies Act and codes such as the King III Report (on corporate governance), provide guidance on how those charged with governance should meet their corporate responsibilities. In practical terms, the effect which those charged with governance have on the control environment will depend on:

* whether they maintain an independent and professional relationship with management

* whether they make good use of the information they receive about the business
* how they deal with difficult issues which may arise
* their experience and stature.

4.1.4 Management's philosophy and operating style.

As we discussed earlier, control environment is largely about management setting an example by their attitude to, and awareness of, the importance of the internal control process. If a manager sets a bad example, or has an overly relaxed approach to control, the employees reporting to him will soon sense that internal control activities and policies are not that important. Whilst successful management may require a level of aggressiveness and risk taking, it should be tempered by an element of conservatism and respect for the need to operate the business within a framework of controls.

4.1.5 Organisation structure.

The organizational structure is the framework within which the entity's activities to achieve its objectives are planned, executed, controlled and reviewed. Obviously the structure will vary considerably from entity to entity, depending on such things as size and activity but in general terms, an effective organizational structure will recognize key areas of authority and responsibility and appropriate lines of reporting. In most companies of reasonable size, this will necessitate a board of directors, divisional or regional management, separate functional sections such as administration and operations, as well as functional cycles such as acquisitions and payments, revenue and receipts, warehousing, payroll, etc. The different combinations are endless, the point is that a good control environment is enhanced by the identification of key areas and clear lines of reporting, so everybody in the organization knows how the entity fits together.

4.1.6 Assignment of authority and responsibility.

This is about making sure that individuals are fully aware of the extent of their authority and how they exercise it, (e.g. making out a document, signing a contract or voting at a meeting) and the responsibilities which they have within their section. It is also about management assigning authority to appropriate individuals according to their function, status in the entity and competence. For example, a clerk in the creditors section should not be signing cheque payments or authorizing electronic funds transfers to creditors. A single individual should not be authorizing the purchase of a R25 million machine (the board of directors should do so on the recommendations of a capital expenditure committee), and a debtors clerk should not be authorizing the write-off of a bad debt. Some transactions within a business may require the authority of the shareholders, e.g. a loan to a director. Obtaining authority for an action or transaction may require that a number of steps be followed and it may involve employees in different functions and at different levels of responsibility. It is also important that in assigning authority and responsibility, overly strict policies and procedures can be counter-productive to a healthy control environment. It can irritate employees, frustrate customers, waste time and squash initiative. This is sometimes referred to as having "too much red tape".

4.1.7 Human resource policies and practices.

We made the point earlier in the chapter that people are an integral part of the internal control process. Perhaps they are the most important. A company which does not have sound policies regarding its human resource (people), will not have a good control environment. Thus the entity should have in place, policies and procedures to:

* recruit the right people: interviews, background checks, minimum qualifications
* train and maintain competence: training courses, workshops, seminars
* determine fair remuneration: industry norms, appraisals of performance, benefits
* develop and promote: training, educating, guidance, career paths
* counsel: suitably qualified, human resource personnel.

4.2 The entity's risk assessment process.

Just as it sounds, this component deals with how the entity assesses the risks which face the entity and how they should be addressed. However, if the ***objectives of the entity are not defined***, the risks of not achieving the objectives cannot be properly identified, assessed and responded to.

Objectives are not applicable only to the entity as a whole, as say, in the strategic plan. Objectives must be set for all departments and functions of the organization and the risks which threaten achievement of the objectives can then be identified, assessed and responded to. For example, the warehouse manager may set the objective of limiting inventory losses to 1% of the average inventory held for the year. Risks which may threaten this are theft of inventory, damage to, or obsolescence of inventory, acceptance of defective inventory from suppliers, poor record keeping of inventory received from suppliers, poor record keeping of inventory movements and so on. Once all of the risks have been identified and assessed, suitable policies and procedures can be put in place to address the risks, e.g. additional competent staff may be employed, physical security may be improved (to prevent theft), inventory cycle counts may be introduced, and the accounting system and supporting documentation may be upgraded.

The risk assessment process involves:
* identifying business risks relevant to financial reporting objectives
* assessing the likelihood and frequency (occurrence) of risks identified
* estimating the potential impact (significance of) if the risk was to occur
* deciding about actions to address the risks.

In a large organization, the risk assessment procedures may be very formal and specific, and the following are very common (in large companies)
* the appointment of risk committees and risk officers
* the engagement of external risk consultants
* the use of risk models
* regular meetings at divisional, departmental and sectional level to consider the risks at those levels
* strategy meetings involving senior management to assess risk at an overall level.

In a small organization, it will be far less formal; in a small business there is neither the time nor the need for complex or formal risk assessment. It is far more likely that management will identify, assess and respond to risk in the natural course of their direct involvement in the business. In a sense, they know the business and will address the risks in the most effective and practical manner they can. Obviously, known or expected risks are easier to respond to, but will still have to be addressed in terms of the resources the entity has available.

4.2.1 Companies classify or describe the risks they face in different ways; strategic risks, financial risks, environmental risks, etc, but for the purpose of understanding risk assessment as a component of internal control, we can describe risks as:

* ***operational risks:*** the risks that threaten the entity, its departments and functions, from achieving effective and efficient operations, e.g. the risk of inventory theft, the risk of individuals gaining access to confidential information, the risk of unauthorized expenditures being made, or the risk of running out of raw materials for manufacture. There are numerous risks.

* ***financial reporting risks:*** the risks that the entity does not achieve its objective of having an accounting system (part of the information system) which records and processes only transactions (and events) which have ***occurred*** and have been ***authorized*** (valid transactions) and which are recorded and processed ***accurately*** and ***completely***, e.g. the risk that fictitious wages will be paid, the risk that unauthorized journal entries will be processed, the risk that discounts and VAT calculations will be incorrectly calculated, or the risk that a sale will not be raised for goods that were dispatched in response to a valid customer order. Again, the risks are numerous.

* ***compliance risks:*** the risks that the entity does not achieve its objective of complying with the laws and regulations applicable to the entity, e.g. taxation, labour, foreign exchange, reporting standards, environmental law, road transport and consumer protection. This time, it is the acts and regulations that are numerous!

4.2.2 Once objectives have been defined, and the risks identified and assessed, the risk can be responded to. The overall response will be for management to:

* ***put in place an information system***, including business processes. These are quite complicated sounding words but essentially:
  - an information system is just a combination of machines (which most often include computers), software where computers are involved, people who carry out procedures, and data
  - related business processes are the activities designed to purchase, produce, sell and distribute the entity's products and ensure compliance with laws and regulations, and record information.

  Clearly the two are interrelated and the distinction between the two can be blurred. Don't let this worry you, think of the two as a combined process/method of initiating, recording, processing and reporting transactions, either manually or through computers or a combination of both.
* ***put in place control activities:*** control activities are the actions, supported by policies and procedures which, if properly designed and carried out, reduce or eliminate a specific risk or risks. Both the information system and business processing are dealt with in the next component.

4.3 The information system and related business processes, relevant to financial reporting.

This component consists of the procedures and records established by the entity to:

* initiate, record, process and report transactions
* capture events and conditions other than transactions (such as depreciation)
* accumulate, record, process and summarise information for the preparation of the financial statements.

The accounting system is part of the information system and is obviously relevant to successful financial reporting.

The objective of the information system and its sub-part, the accounting system, is to produce information which is ***valid*** (the transactions and events underlying the information actually ***occurred*** and were ***authorized***), ***accurate*** and ***complete***, and timeously produced. No doubt these objectives can be expressed differently but in effect what the business wants its accounting system to do, whether it is manual or computerized, is to produce information which displays these characteristics and is produced promptly enough to be useful. For example, when the sales director looks at the sales figures for the month, he wants to be reasonably sure that the sales that are included in the total, have actually been made and that the figure does ***not*** include fictitious sales. He also expects the sales to have been at the correct selling price, discounts given to have been authorized, and all casts, extentions and VAT calculations to be correct. He will probably also assume that the sales were made ***only*** after the creditworthiness of the customer had been checked. Lastly the sales director requires the information promptly, not three weeks later when it is too late for him to react to the information, and take any remedial action.

So, is the information system with its machines, people, documents and data, a sufficient response on its own, to the risk that the financial information it produces may ***not*** be valid, accurate and complete? The answer is no, the fourth component of internal control must be added and that is termed the control activities component.

4.3.1 The information system will need to define and provide the machines, documents, ledgers and procedures which will guide the entity's transactions through the system. This will include:

* ***initiation*** of the transaction, e.g. receipt of a customer's order over the phone or through the post
* ***recording*** the transaction, e.g. entering the details of the customer's order on an internal sales order
* ***processing*** the transaction, e.g. picking the goods ordered from the warehouse and dispatching them to the customer and raising the sale by preparing a sales invoice
* ***posting*** (transferring) the transaction to the general ledger, e.g. this will usually involve entering the invoice in the sales journal and posting (transferring) amounts and totals to the general ledger accounts (sales and accounts receivable) and the debtors ledger

Within this process there will be procedures to ***correct*** errors which may occur, e.g. correction of invoices made out using incorrect prices.

As pointed out above, the activities may take place in a manual or computerized environment. The vast majority of systems will be a combination of the two.

4.3.2 Books and documents.

All of the actions described above will be supported by ledgers, journals, records and documents specific to the type of transaction, e.g. a sale should be supported by a customer order, an internal sales order, a picking slip used to select goods, a dispatch (delivery) note and an invoice. There should be a sales journal and a debtors ledger as well as the general ledger. (Documents used in all the major cycles are described in the subsequent "cycle chapters" of this text).

4.3.3 Document design.

Properly designed documents can assist in promoting the accuracy and completeness of recording transactions:

* pre-printed, in a format which leaves the minimum amount of information to be manually filled in
* pre-numbered; consecutive pre-numbering facilitates identification of any missing documents either at the recording stage or subsequently e.g. a clerk listing goods received notes at the end of a week may discover that certain GRNs are missing
* multi-copied, carbonised and designed for multiple use, e.g. a sales clerk taking an order from a customer over the phone should complete only the top copy of the sales order; the first carbon copy of the sales order could then be used by stores as a "picking slip" to select the goods picked, and the second carbon copy sent to accounting. In addition each copy should be a different colour for easy identification
* designed in a manner which is logical and simple to complete, e.g. key pieces of information required to execute the transaction should have a prominent position on the document. A very important piece of information on a sales order would be the customers account number, hence the sales order should display quite clearly the necessary space into which the account number can be entered. Further good design may be to break the account number space into a series of small blocks totalling the number of digits in the account number. This enhances the chances of the complete account number being recorded
* contain blank blocks or grids which can be used for authorising or approving the document e.g. a blank block for the preparer of the document to sign and a blank block for the person who checked the document to sign. This characteristic facilitates isolation of responsibility.

Obviously these characteristics relate primarily to manual systems but remember that the majority of computerized systems still use hardcopy documents. The computer may produce the document itself but the principles remain the same. As you will see when you study computerized controls, programmed controls (automated controls) can enhance accuracy and completeness considerably.

4.3.4 Events and conditions other than transactions.

The vast majority of an entity's activities are reflected in transactions, e.g. selling goods, purchasing goods, paying salaries and wages and incurring capital expenditures. There are, however, other events and conditions which must ultimately be reflected in the financial statements either within ***account headings*** such as depreciation, impairment, bad debt allowances, inventory obsolescence allowances or as ***disclosure*** in the notes to the financial statements, for example, the inclusion of a contingent liability which may have arisen. Generally, these types of event will need to be separately considered and authorized by senior management and will frequently be recorded by journal entry. It will be the responsibility of the senior financial personnel to ensure that these matters are identified. A checklist of month end or year end "matters to consider" may be used, or specific meetings with a standardized agenda to deal with these matters, may be scheduled.

4.3.5 Journal entries.

Many journal entries are routine in nature and simply facilitate the recording of monthly totals in the general ledger, or adjustments which management wish to make, e.g. write off

a bad debt. The point of the matter is that journal entries alter the balances in the general ledger and thus can be used to manipulate financial information and conceal irregular or fraudulent activities. This risk should be addressed by the information systems and particularly by the control activities related thereto. The emphasis should be on authorization of the journal entry by a "more senior" level employee.

4.4 Control activities.

These are the actions, supported by policies and procedures which are carried out to manage or reduce the risks that the objectives of the organization will not be met. For example, the policy of the entity may be that credit exceeding R50 000 will not be extended to any customer. The procedure may be that every new customer must submit a credit application with sufficient information for the entity to establish the applicant's creditworthiness by following up on the information provided. The action may be that before a sale is made to that customer, the salesperson checks the status of the customer's account to ensure that the sale will not push the customer beyond the R50 000 credit limit. This "package" of action, policy and procedure is a control activity designed to address the risk that the entity's objective of limiting losses from debtors who may not pay. Control activities are closely linked to the information system and meeting the objectives of processing ***accurately*** and ***completely*** only transactions which have ***occurred*** and have been ***authorized.*** To illustrate the point, consider the following:

An accounting system is a series or collection of tasks and records by which transactions are processed to create financial records. An accounting system identifies, assembles, analyses, calculates, classifies, records, summarises and reports transactions and other events. The major elements of the accounting system are ***people*** who carry out ***procedures*** e.g. write out a credit sales invoice, calculate a price, enter the invoice in a sales journal, etc, and ***paper*** such as order forms, ledgers, lists, invoices etc, which facilitate the initiation, execution and recording of the transaction. (Of course even at this early stage, you should realise that computers can be, and are used to replace people and paper and to perform procedures, but that will be dealt with in later chapters.)

Management must now add ***control activities (actions)*** to the accounting system if it is to produce financial information which is representative of transactions which have occurred and were authorized and which is accurate and complete and which is timeously produced. In the paragraph above, we indicated that an employee writes out an invoice, calculates a price, enters the invoice in a sales journal etc. This is the ***accounting system***. Management now adds ***control activities***; before the invoice is written out, the salesperson checks that the customer is a valid account holder and that the customer is not behind on his payments and will not be exceeding his credit limits; a second salesperson may check the invoice to ensure that pricing, discounts and VAT calculations are correct. At a later stage, an accounts clerk may confirm that all invoices for the week have been entered into the sales journal.

There are numerous control activities with different objectives and which are applied at different organizational levels and functions. Control activities can also be described as follows:

Description A: type of control activity
Description B: preventive, detective or corrective control activities
Description C: general and application control activities

Description A: type of control activity

4.4.1 Approval, authorization

Management authorizes employees to perform certain tasks within certain parameters, e.g. making a sale on credit may require the approval of the credit controller. Management gives the credit controller the authority to authorize the sale but only after the creditworthiness of the customer has been checked. The level of authorization may vary for different transactions and may be more onerous for some than for others, e.g.:

* a payment by cheque should require at least two signatories to authorize the cheque
* payments over R250 000 paid by electronic funds transfer may only be authorized by the financial director and the most senior accountant
* a loan to a director must be authorized by the shareholders in terms of the Companies Act

* the acquisition of an expensive piece of equipment may first require budget approval (if it is not in the budget, it can't be purchased), followed by approval of the production manager.

Authorisation of a transaction is not just a matter of signing a document. ***Before*** the approval/authorization is given, supporting documentation and/or other evidence must be checked to ensure that the transaction is valid. A cheque signatory should not just sign a cheque which is put in front of him, he should check the documentation carefully. A foreman who is authorizing overtime hours worked, by signing a clockcard or schedule of overtime, must satisfy himself that the hours recorded as overtime were genuinely worked. This principle of "checking before authorizing" is simple and logical but often does not happen. The employee whose duty it is to authorize may be too busy, too trusting or too lazy!

4.4.2 Segregation (division) of duties

Segregation of duties is essential for effective internal control as it plays a major role in reducing the risk of errors and illegal or inappropriate actions occurring. The principle is that the various actions or procedures that are carried out in respect of a transaction should be divided amongst the employees, and that the custodian of the entity's assets, should not be responsible for the records relating to the asset. Segregation of duties also facilitates the checking of one employee's work by another employee.

If we broadly categorise the functions surrounding a transaction, we come up with the following: (the example has been simplified for illustrative purposes)

Function	***Example***
Initiation and approval	A purchase order is authorized
Executing	The order is placed with a supplier
Custody	The goods are delivered and placed in the warehouse
Recording	The purchase is entered into the accounting records and the perpetual inventory records are updated

Let's assume for example, that Clarence Carter is responsible for all of the functions above. He could very easily purchase goods for himself which will be paid for by the company. He will have access to an official company order so he can order the goods he wants and, as he is also placing the order, he can choose whichever supplier he likes (the supplier could even be his own business run by his wife). As Clarence Carter is also responsible for taking delivery of the goods, he will make out the necessary document (goods received note) when the goods are delivered. He now has the goods in his possession and can take them home. If he also updates the perpetual inventory records, he can ensure that the records agree with the physical inventory (in case anyone checks) by not recording the goods purchased or by writing up a fictitious goods issue. It will be even easier if there are no perpetual inventory records. With regard to paying for the goods, the necessary documents will be there to support the payment, e.g. a signed purchase order, a supplier delivery note, a goods received note and a supplier invoice. So even if Clarence Carter is not involved in the actual payment of the supplier, there is no reason that the goods will not be paid for. Obviously, if Clarence Carter is really devious, he will restrict his fraudulent purchases to items which the company itself normally purchases so as not to draw attention to the purchase. For example, if he works for a garden

tool wholesaler and orders himself a big screen TV, it will be difficult for the transaction not to be noticed. However, if he buys garden tools for his own use or which he intends to sell to make some extra cash, the transaction will not appear out of the ordinary.

The idea behind segregation of duties is that other employees are introduced into the functions surrounding the transaction. In a large organization with the necessary resources, the purchase transaction would be divided up as follows:

(i) ***initiating and approving the purchase***: this would be the responsibility of the warehouse department who would produce an authorized (signed) stores requisition, describing accurately the goods to be purchased. The requisition would be approved by the warehouse manager, based on an inventory re-order level or production schedule.

(ii) ***executing the order***: the requisition would be sent to the (separate) order department where an employee would make out the purchase order and place the order with an approved supplier. Another more senior employee (such as the chief purchases officer) would approve the order before it is placed.

(iii) ***custody***: in the custody function, warehousing would be a separate function and would be broken down into three sub-functions, i.e. receiving the goods from the supplier, looking after the goods in the warehouse, and issuing of goods. (In this example we are not dealing with the issuing of goods from the warehouse.) Each of these sub-functions would be carried out by different employees who are not involved in other functions.

(iv) ***recording***: recording of this purchase will take place in another separate section, i.e. the accounting department. Different employees within the section will be responsible for the recording of purchases and raising of creditors and for maintaining the perpetual inventory. The process of actually paying the creditors is, in effect, another "transaction" and will be subject to its own segregation of duties.

(v) ***review:*** where there is good segregation of duties, an additional function will be carried out, i.e. independent review/reconciliation by management.

What this example of good segregation of duties illustrates is that Clarence Carter would not be able to purchase goods for himself and have the company pay. His biggest problem would probably be getting his hands on the goods he has ordered. Even if he could get hold of a purchase order and place an order with the supplier, he still has to obtain the physical goods. Remember that once the goods have been delivered, the receiving clerk and the storeman can be held accountable, so they are going to make sure they carry out their duties properly. On top of that, the accounting section is keeping an ***independent*** record of what inventory should be on hand. The storeman will want to make sure that his physical inventory agrees with these records and management will be carrying out ***reviews*** to see if the physical inventory and the inventory records, do agree. In effect, each step in the process of making a purchase, has been allocated to a different employee and the next employee in the process is checking on the previous employee.

In a perfect situation all of the functions above would be segregated, but due to factors such as cost and insufficient employees, it is frequently not possible. So which of the divisions are most important? Generally speaking, "custody" and "recording" are the most incompatible. The reason for this is that if an individual has ***control*** of the asset and ***keeps the records*** pertaining to the asset, the record of the asset can be made to agree with the physical assets on hand. For example, a storeman who has access to the inventory and the perpetual inventory records, can steal inventory and alter the records to ensure that the theoretical inventory on hand agrees with the physical inventory. The same logic can be applied to other physical assets such as equipment. The employee in charge could steal equipment and manipulate the fixed asset register. What about the company's bank account? The custodian of the bank account is the employee who has the power to sign cheques or effect electronic funds transfers. If this individual also writes up the cash journals, he can make whatever payments he likes and describe them

in the cash payments journal as valid business payments. If the credit controller (who is the custodian of the company's debtors), is able to make adjusting entries to the debtors ledger, he will be able to invalidly write off the debt of a friend or customer so that they don't have to pay. If custody and recording are not segregated, the effectiveness of "review" is diminished as the physical and theoretical will be easily reconciled.

Segregation of duties is not aimed solely at safeguarding the assets of the business. It is a very effective technique to ensure that transactions are recorded and processed accurately and completely and that only transactions that actually occurred and were authorized are recorded and processed. In effect, segregation of duties provides a series of independent checks on whether employees are doing their jobs properly.

The biggest enemy of segregation of duties, is ***collusion***. As we discussed under the limitations of internal control, segregation of duties (and other control activities) can be circumvented if management or employees collude (work together) intentionally with other individuals inside or outside the company. For example, if the storeman and the keeper of the perpetual inventory records collude, they will be able to cover up inventory theft. Essentially if one employee in the process agrees, for whatever reason, not to check the action of another employee who he is supposed to check, segregation of duties breaks down. Collusion will frequently be with parties outside the organization, a buyer colludes with a supplier to charge the company a higher price and later they share the proceeds, or as described earlier, a receiving clerk colludes with a supplier's driver and the storeman to accept a short delivery as a full delivery. The driver will then sell the goods which should have been delivered, and share the proceeds with the receiving clerk and the storeman. This will be even easier if a person who has access to the perpetual inventory records is included in the scam.

Good segregation of duties starts by dividing the company's cycles, e.g. acquisitions and payments, payroll, into functions and then further segregating the duties within the function. (See chapters 10 – 14.)

4.4.3 Isolation of responsibility

For any internal control system to work effectively, the people involved in the system must be fully aware of their responsibilities and must be accountable for their performance. It is equally important that the employees acknowledge in writing, that they have performed the task or control procedures necessary to fulfil their responsibility. This is usually done by signing. Once a document is signed it isolates the employee who was responsible for carrying out some control activity. A signature also isolates a transfer of responsibility from one person to another. For example, when a supplier delivers goods to a company, the company's receiving clerk should count the goods received and ***sign*** the supplier's delivery note, a copy of which is kept by the company. This signature fulfils two important functions; firstly if there is a subsequent problem with the delivery, management can ***isolate*** who was responsible for receiving the delivery, and secondly, the signature ***acknowledges*** the physical transfer of the goods and responsibility therefore, from the supplier to the purchaser. Other examples will be, the foreman signing a schedule of overtime to approve it, or the chief buyer signing an order to acknowledge that the detail of the order has been checked, it is supported by a signed requisition and the supplier to whom the order will be sent, is approved by the company.

4.4.4 Access/custody (security)

Control activities will include actions, policies and procedures which protect the company's assets. Again, assets must be thought of in the wider context, not just physical assets such as inventory and plant and equipment. The company will also have cash in the bank, perhaps investments and certainly debtors, for all of which there is no physical asset but simply "entries in the books." The company will also have important documents and confidential information which must be safeguarded. Access/custody controls are designed to:

* prevent damage to, and deterioration of, physical assets e.g. by proper storage and treatment of such assets

* prevent deterioration of certain "non-physical" book assets e.g. controls to ensure that debtors don't get behind in their payments
* prevent unauthorised use, theft or loss of physical assets e.g. by proper security measures
* prevent unauthorised use, theft or loss of "non-physical" book assets, e.g. by limiting the number of personnel who have signing powers to transfer cash or sell investments, and by protecting the debtors ledger from being altered or destroyed.

4.4.5 Comparison and reconciliation

A reconciliation is a comparison of two different sets of recorded information or of recorded information and a physical asset, for example:

* the cash journal to the bank statement
* the individual creditor's accounts to creditors statements
* subsidiary ledgers to the general ledger, e.g. the debtors ledger to the general ledger
* physical inventory and plant and equipment to the perpetual inventory and asset register respectively
* the wage expense from one wage period to the next.

There are any number of reconciliations which can take place but the object of comparison and reconciliation is to ***identify, investigate*** and ***resolve*** differences where necessary. There is no point in simply performing the mechanical reconciliation of quantities or amounts without investigating and resolving the reconciling items.

Comparison is also not that useful on its own. If a comparison of actual expenditure on overtime compared to budgeted overtime reveals that the budget has been exceeded, the overspend must be followed up and remedial action taken.

4.4.6 Performance reviews.

As a control activity, reviews of performance provide a basis for identifying problems. When carrying out a review, the reviewer is looking for consistency and reasonableness in the data being reviewed. Unexpected results or unusual conditions will then be followed up. Review as a control will usually be carried out by employees in management or supervisory positions and may include review of:

* performance against budgets, forecasts, departmental targets, etc
* key performance indicators, ratios, etc
* current to prior period, financial or operating information.

For example a review of the key performance indicators may reveal that the gross profit percentage has declined sharply. The follow up may reveal that breakdowns in the custody controls for inventory have occurred, resulting in the theft of inventory.

Description B: preventive, detective or corrective control activities.

4.4.7 ***Preventive*** controls are controls which are put in place to prevent or minimize errors or illegal events from occurring. They can be regarded as proactive actions or procedures designed to prevent a loss. Types of preventive control activities are physical controls over assets (custody controls), approval and authorization, and segregation of duties. Examples of specific preventive controls are all cheques to be signed by two authorised employees, EFT payments can only be effected from certain terminals and require additional unique passwords to be entered, the chief buyer signing a purchase order before the order is placed, valuable inventory items being stored in a locked enclosure within the warehouse, and keeping blank (unused) company documentation under lock and key, e.g. cheque books, credit notes, etc.

4.4.8 Detective controls.

As we have discussed earlier in this chapter, internal control activities are not foolproof and not all errors will be prevented. There may be collusion or employees may be careless or want to take short cuts. Detective controls are like a "second line of defence" and are designed and implemented to identify the errors, thefts, omissions, etc, which got through the "first line of defence". Reconciliations and reviews are common types of detective control activities but segregation of duties (e.g. one employee checking another) as well as custody controls have a detective element to them.

4.4.9 Corrective controls.

These are controls which are implemented to resolve errors and problems which have been identified by detective controls. For example, if the accounting department "detects" an invalid charge from a supplier (an invoice for goods which were not actually received), what procedures must be followed to rectify the situation and ensure that the invoice is not paid and that the same problem does not keep happening?

Although control activities can be classified in this manner in manual accounting systems, the classification into descriptions is more relevant and defined in computerized accounting systems. Because computers can process vast quantities of transactions at lightening speed and invisibly, ***preventing*** unauthorized or erroneous transactions from entering the system is very important, and because the consequences of not doing so can be extreme, ***detective*** controls are also very important as the problem causing the errors etc must be ***corrected*** very quickly. In addition, the capabilities of the computer and its software allow a wide range of preventive and detective controls to be implemented. These are discussed in chapter 8.

Description C: General and application control activities.

ISA 315 (revised) lists, under control activities, policies and procedures that pertain inter alia, to "information processing". It then states that two broad groupings of information systems control activities are ***application*** controls and ***general*** controls. The classification of controls into ***general*** and ***application*** controls emerged originally from computerised environments and are not terms that are generally used in manual accounting systems. Strictly speaking, general and application controls go beyond the "control activities" component of the internal control process. They touch to an extent, all of the other components. This will become clear to you when you study general and application controls. These controls are dealt with in chapter 8, but a simple distinction between the two would be that general controls are those which establish an ***overall*** framework of control for a computerised environment at large. These are controls which should be in place before any initiating recording, processing or reporting of transactions takes place. Application controls are controls which are specific to a particular task, e.g. preparing the payroll. Controls such as restricting access to the computer centre would a general control, whilst a programmed (automated) control which prevents an incorrect employee number from being included on the payroll, would be an application control. Application controls can be directly linked to the control activity component.

4.5 Monitoring of controls.

The final component of internal control is monitoring. This involves the assessment of internal control performance ***over time.*** Remember that management sets up internal controls with the intention of reducing the risks that the entity's objectives will not be met; ***monitoring*** is the component of the process which tells management how they are doing. Successful monitoring is achieved by ongoing assessment by management itself, supervisory staff such as department heads or "independent" bodies such as internal audit or risk committees. Monitoring of the internal control process is not only about determining whether the control activities are actually taking place; it is also about determining whether the controls are ***effective***. Monitoring can take place in various ways.

Example 1. The internal audit department of Permo Ltd, checks on a random but regular basis, whether bank reconciliations are accurately and timeously carried out.

Example 2. Permo Ltd installed closed circuit TV cameras in its receiving bay and warehouse in an attempt to reduce theft of inventory. The operations manager analyses inventory movements independently over a period of time to determine whether loss from theft of inventory has declined. If not, the cameras are not proving to be an adequate response to the risk of theft, and other control activities will have to be introduced.

Example 3. Ruiz CC has control activities in place to reduce losses from bad debts. By monitoring the amounts written off over time, management can assess whether the controls are effective.

Example 4. Costa TV Ltd a service provider, has a phone in line which customers can call if they are unhappy with the company's fee charging, e.g. incorrect amounts invoiced. Calls are recorded and monitored by the service manager, particularly the number and nature of the complaints.

Example 5. Chemicalplus Ltd, engages an environmental expert to monitor the government pollution index with which the company must comply. Substantial fines are payable for failing to meet the government requirements.

The important point about monitoring the internal control system is that if it is not carried out, neither the board nor management will know whether:

* the entities financial reporting is effective
* operations are being effectively and efficiently conducted
* the entity is complying with applicable laws and regulations.

Although internal control consists of the five components (4.1 to 4.5) discussed above, the system itself is a process; the components are not independent of each other. To be effective as an internal control system, the components must all work together. For example, if there is a poor control environment, it is unlikely that the control activities will be effectively carried out. In theory, the information system may be well designed and appropriate control activities may be stipulated, but if the control environment is one of "don't worry too much about controls", the information system and control activities will not be effective. Similarly, inadequate identification and assessment of the risks facing the entity will result in an inadequate system with insufficient control activities. A well designed system which is not monitored over time, will also become ineffective.

5. INTERNAL CONTROL IN SMALLER ENTITIES

You will probably have worked out that internal control as described in these preceding pages, will suit large companies far better than smaller entities. There are a number of reasons for this:

5.1 Control environment

* the control environment in a smaller entity will depend virtually entirely on the tone and control consciousness set by management
* in a smaller entity, management and the lower level employees will be working closely together so employees will frequently be exposed to how managers behave and conduct themselves. The positive side of this is that managers can have a strong and direct influence on the employees with whom they work, and can play a far more direct role in control activities
* there is no reason that a smaller entity cannot be committed to competence but putting it into practice may not be as easy. Firstly, due to lack of staff numbers, employees may find themselves responsible for activities for which they do not have the necessary skills and knowledge and which they are not quite competent to perform. Secondly, there may not be the necessary resources to attract and retain the best staff. Frequently in smaller entities there will not be a separate human resource manager, so the implementation and management of comprehensive human resource policies and practices is difficult and activities such as recruiting, training, counseling, etc, will suffer
* organizational structures and the assignment of authority and responsibility will be negatively affected by the lack of employees at different levels of authority. This is partially countered by the more direct involvement of management in the day to day operation of the entity
* generally in smaller entities, there is far less distinction between the board of directors and management, frequently they are the same individuals. There will probably be no non-executive directors and as a result that independent oversight "check" on management is not possible. If there is no oversight of management by those charged with governance, the control environment will be weakened.

5.2 Risk assessment process

* with regard to the risk assessment process, it is most unlikely that there will be risk committees, risk officers or formal risk assessments. Managers and staff in smaller entities do not have the time for this (perhaps they should make time!) and the entity will not have the resources. The assessment of risk in a small entity is far more likely to be an informal process carried out by managers and others as they go about their daily duties.

5.3 The information system

* as for the "information system and related business processes" component, a smaller entity is more likely to have a simple accounting system under the charge of an accountant and a small number of assistants who run the entire system and which produces basic financial information. This does not mean that the financial information will be poor, but there are likely to be far less control activities in place to reduce the risk of unauthorized transactions, inaccurate or incomplete recording, etc. On the positive side, there is no reason that a smaller entity should not make use of good, well designed documentation and reputable accounting packages which produce reliable information to meet the financial reporting needs of the entity.

5.4 Control activities

* implementing control activities can be expensive and smaller entities may not have the necessary resources to put in more effective but costly security controls or employ that extra individual to improve segregation of duties
* smaller entities carry out fewer transactions (fewer sales, fewer purchases) and consequently some employees may be involved in more than one cycle and invariably will carry out incompatible functions within a cycle. For example, the storeman may act as the receiving clerk, the custodian of inventory and the dispatch clerk, and may even maintain the inventory records.
* segregation of duties is a fundamental control activity and without it other control activities will be weakened or will not be possible. The simple control of one employee checking the work of another becomes very difficult to implement. Usually there will not be multiple levels of employees within a cycle or even within the entity. There will be no junior purchase officer, senior purchase officer and chief purchasing officer. Just a purchase officer who may even be responsible for initiating, approving and executing a purchase order.

5.5 Monitoring

* monitoring of the internal control process in a smaller entity will again be left up to management, and will be carried out informally. It is unlikely that there will be an independent internal audit department, reviews by external bodies or customer hot lines! Furthermore, as the directors are probably involved in day to day operations, there will be little independent monitoring of facts, figures and performance. On the positive side, this direct involvement should give management a good ideal of whether the process is working successfully.

  Do not get the impression that all small entities have weak internal control as this is simply not the case. There are many smaller entities with outstanding internal control systems. Good systems design, competent and dedicated employees, combined with ethical and "hands on" management, can far outweigh the disadvantages of being a smaller entity.

6. THE EXTERNAL AUDITOR'S INTEREST IN INTERNAL CONTROL

The external auditor is primarily interested in the fair presentation of the entities annual financial statements. The financial statements are a product of the entity's information systems which includes the accounting system. It stands to reason therefore that the better the internal control process, the more likely it is that the financial statement will be fairly present.

ISA 315 (Revised) – Identifying and assessing the risks of material misstatement through understanding the entity and its environment, requires that the auditor obtain an understanding of the entity's internal control and suggests that a good way of doing this may be to evaluate the five components of internal

control. For example, ISA 315 (Revised) states that the auditor should identify and assess the risk of material misstatement occurring in the financial statements so where the entity itself has a risk assessment process, it makes sense for the auditor to understand the entity's process and benefit from it in obtaining knowledge about the risks faced by the entity. Similarly, an assessment of the entity's control environment will significantly influence the auditor's assessment of the risk of material misstatement in general and will in turn directly affect how the audit is conducted. An understanding of the information systems and control activities is equally important for the auditor as, without understanding these, the auditor is unable to properly assess the risk that management's objective of producing valid, accurate and complete financial information will be achieved. Finally, if the internal control process is properly monitored, the auditor may be in a position to work with the monitoring bodies such as internal audit and will at the very least, be able to derive benefit from the results of the monitoring and how and whether issues in which the auditor is interested, have been addressed.

AUDIT EVIDENCE

1. INTRODUCTION

Audit evidence is absolutely fundamental to the audit function. As was explained in Chapter 1, the auditor has a duty to gather evidence to support his opinion on whether the assertions of the directors, embodied in the annual financial statements, are fairly presented. ISA 500 – Audit Evidence, states that "the objective of the auditor is to design and perform audit procedures in such a way as to enable the auditor to obtain sufficient, appropriate audit evidence to be able to draw reasonable conclusions on which to base the auditor's opinion." The key to this standard is the phrase ***"sufficient, appropriate evidence"***.

2. SUFFICIENT APPROPRIATE AUDIT EVIDENCE

2.1 Sufficient evidence

The sufficiency of audit evidence relates to the ***quantity*** of audit evidence gathered. The auditor must evaluate whether enough evidence has been obtained to support an opinion. This is a particularly important decision as auditors do not examine every transaction, but rather perform procedures on samples of populations; for example, if an auditor is performing tests of controls on the acquisitions cycle to establish whether all purchases were authorised, how many purchase requisitions or purchase orders should be inspected for an authorising signature, to enable the auditor to draw a conclusion on whether the authorization control operates? Similarly, when testing the existence of debtors, how extensive should the positive debtors circularization or subsequent receipts testing be, for the auditor to be in a position to draw a conclusion on the existence assertion for debtors?

The question of sufficiency is further complicated by the fact that evidence about an assertion is not gathered by performing a single procedure, but by performing a number of procedures each of which contribute some evidence. Evidence is cumulative in nature. For example, evidence relating to the existence of debtors can be gathered by performing a debtors circularisation ***and*** by testing subsequent receipts from debtors. (This procedure involves tying payments received from debtors ***after*** the reporting date to amounts owed by those debtors ***at*** reporting date and is based on the premise that if a debtor pays, it is strong evidence that the debtor existed.) The auditor has to balance the extent of each procedure performed.

There is no hard and fast way in which the quantity of audit evidence needed can be precisely calculated. It is a very subjective decision requiring a strong dose of professional judgement. Certainly there are statistical models which can assist in determining sample sizes, but even these models require the auditor to make some subjective decisions. The quantity of audit evidence relates to the "extent of testing" which is a component of the audit plan (the other two being the nature and timing of tests). The audit plan is only decided upon once the full exercise of devising the overall audit strategy has taken place. The planning process also includes making subjective decisions e.g. evaluating risk, so the auditor is really left with using his professional expertise to determine whether, in the light of the prevailing circumstances surrounding the audit, enough evidence has been gathered.

2.2 ***Appropriate evidence***

The appropriateness of audit evidence relates to the ***quality*** of audit evidence. This can be further broken down into the ***reliability*** (source and nature) of the evidence and the ***relevance*** of the evidence to the assertion which is being audited.

* ***Reliability***

Some evidence is simply more reliable than other evidence. The hierarchy of reliability for audit evidence can be expressed as follows:

- evidence ***developed by the auditor*** is the ***most reliable*** source, e.g. the auditor inspects inventory to obtain evidence of its existence
- evidence provided directly by a ***3rd party*** to the auditor (as opposed to the client) is ***reasonably reliable*** evidence, provided that the 3rd party is ***independent*** of the client, ***reputable*** and ***competent*** e.g. information obtained from the client's attorneys.
- evidence obtained from a ***3rd party*** but which was ***passed through the client*** is ***less reliable*** as the client may have had the opportunity to tamper with the evidence e.g. a bank statement or certificate of balance which is not sent directly to the auditor.
- evidence generated through the client's system will be more reliable when related internal controls are effective
- evidence provided by the ***client*** is the ***least reliable*** as it lacks "independence" i.e. it is provided by the persons who are responsible for the assertion for which the evidence is required.
- ***written evidence*** (whether paper or electronic) is considered ***more reliable*** than ***oral evidence*** as oral evidence is easily denied or misinterpreted.
- evidence provided by original documents is more reliable than evidence provided by photocopies or facsimiles.

Clearly the auditor will have to rely on evidence from all of the above sources, (e.g. developed by the auditor, provided by the entity, provided by a 3rd party) and would therefore not reject evidence solely on the grounds of its source. Indeed, even evidence provided by the client may be very reliable, particularly if the accounting systems and internal controls are strong and the directors and employees are competent, reliable and trustworthy. It follows that the hierarchy should be regarded as a guideline.

* ***Relevance***

The ***relevance*** of audit evidence means its relevance to the assertion which is being audited. It is very important that the auditor understands exactly to which assertion the evidence being gathered, relates. If this is not understood, incorrect conclusions will be drawn. For example, when the auditor selects a sample of inventory items from the inventory records to count and inspect at the annual inventory count, he obtains evidence of the ***existence*** of that inventory and (possibly) some evidence of the physical condition of the inventory. The physical condition is relevant to the ***valuation*** assertion as it provides evidence relating to the reasonableness of the allowance for obsolete inventory. However, the inspection of inventory does ***not*** provide evidence to support the ***rights*** assertion applicable to that inventory – simply because the auditor has counted and inspected the inventory in the client's warehouse does not mean that the client has the rights (ownership) to that inventory. It may be inventory held on consignment on behalf of another company or it may be inventory which has been sold, but not yet collected by, or delivered to, the purchaser. Similarly this test will not provide any evidence relevant to the ***completeness*** of inventory. The test for completeness requires that the items be selected from the physical inventory and traced to the records to determine whether they have been included in the records.

When performing tests of controls, the auditor attempts to determine whether the major objective of the accounting system and related internal control, to produce ***valid***, ***accurate*** and ***complete*** information, is being achieved. In doing this the auditor obtains evidence relating to the ***occurrence***, ***accuracy, cut-off, classification*** and ***completeness***

assertions relating to transactions processed through that accounting system. Again, the auditor must be quite sure as to which assertion the procedure being performed (and the evidence gathered from the procedure) is relevant. For example, the auditor may deduce from the tests of controls, that the controls for the recording of sales at the proper amount (***accuracy***) are sound, however, this does ***not*** provide evidence that all sales actually made, were recorded (***completeness***) or that all sales recorded, were genuine sales i.e. not fictitious (***occurrence***).

Finally, a single procedure will not necessarily be relevant to only one assertion, the procedure may provide evidence relevant to a number of assertions.

2.3 Influencing factors in determining whether sufficient, appropriate evidence has been obtained

Whilst the decision as to whether sufficient, appropriate evidence has been gathered, cannot be precisely measured (it remains a matter of professional judgement), the following factors will influence the auditor in making the decision:

* ***the significance of the potential misstatement in the assertion*** and the likelihood of the misstatement having a material effect on the financial statements. It stands to reason that if there is a high risk of material misstatement relating to a particular assertion, ***more*** evidence from the ***most reliable*** source available would be required by the auditor.

* ***the materiality of the account heading being examined***. For example, if inventory is a very material figure in the financial statements, the auditor will be more concerned about obtaining sufficient, appropriate evidence for the assertions relating to inventory, than for those relating to a far less material account heading. Simplistically, the reason for this is that material misstatement in a material account heading will have a material effect on the financial statements. The auditor is likely to seek more evidence of the most reliable evidence available.

* ***experience gained during previous audits***. As the auditor develops a relationship with his client, knowledge of potential problem areas will help to guide the auditor in where to focus the audit.

* ***results of audit procedures already conducted***. For example, if the auditor's initial positive circularization tests on the existence of debtors prove successful, he may decide to perform less additional subsequent receipts testing on debtors than planned. The opposite situation may also arise.

* ***source and reliability of information available***. Clearly the auditor will want to use the best evidence available; however, if reliable evidence is not available, the auditor may be forced to gather more corroborative evidence from a number of less reliable sources to be in a position to form an opinion on a particular assertion. Bear in mind however, that simply gathering more ***unreliable*** evidence is not very helpful.

* ***the persuasiveness of the audit evidence***. For example, evidence gathered on one section of the audit which is supported or corroborated by evidence from another section of the audit will be more persuasive than had the evidence contradicted itself or if there had been no corroborating evidence.

2.4 Audit procedures for obtaining audit evidence

Audit evidence to draw reasonable conclusions on which to base the auditor's opinion is obtained by performing

* risk assessment procedures and
* "further" audit procedures, which comprise
  - tests of controls and
  - substantive procedures, including tests of detail and substantive analytical procedures.

These are discussed further later in this chapter and in Chapter 6.

3. FINANCIAL STATEMENT ASSERTIONS

In Chapter 1 the importance of financial statement assertions was discussed. This chapter revisits the topic in an attempt to confirm the link between the assertions and sufficient, appropriate evidence. The objective of an audit is for the auditor to express an opinion on whether the financial statements are fairly presented. The financial statements are nothing more than an embodiment, in a prescribed format, of the ***assertions*** of the directors to the shareholders concerning the financial position and results of operations of the company they are managing on behalf of those shareholders. As defined by ISA 315 (revised) the assertions are the representations by management, explicit or otherwise, that are embodied in the financial statements, as used by the auditor to consider the different types of potential misstatement which may occur. The statement stipulates the following three categories of assertions:

* assertions about ***classes of transactions and events*** for the period under audit e.g. sales, purchases, interest received
* assertions about ***account balances*** at year-end e.g. accounts receivable, property, plant and equipment, accounts payable
* assertions about ***presentation and disclosure*** e.g. notes which support account headings, contingent liabilities.

3.1 Assertions about classes of ***transactions and events*** for the period under audit:

1. ***Occurrence*** – transactions and events that have been recorded, have occurred and pertain to the entity.
2. ***Completeness*** – all transactions and events that should have been recorded, have been recorded.
3. ***Accuracy –*** amounts and other data relating to recorded transactions and events, have been recorded appropriately.
4. ***Cut-off*** – transactions and events have been recorded in the correct accounting period.
5. ***Classification*** – transactions and events have been recorded in the proper accounts.

3.2 Assertions about ***account balances*** at the period end:

1. ***Existence*** – assets, liabilities and equity interests exist.
2. ***Rights and obligations*** – the entity holds or controls the rights to assets, and liabilities are the obligations of the entity.
3. ***Completeness*** – all assets, liabilities and equity interests that should have been recorded, have been recorded.
4. ***Valuation and allocation*** – assets, liabilities, and equity interests are included in the financial statements at appropriate amounts and any resulting valuation or allocation adjustments are appropriately recorded.

3.3 Assertions about ***presentation and disclosure***

1. ***Occurrence and rights and obligations*** – disclosed events, transactions, and other matters have occurred and pertain to the entity.
2. ***Completeness*** – all disclosures that should have been included in the financial statements, have been included.
3. ***Classification and understandability*** – financial information is appropriately presented and described, and disclosures are clearly expressed.
4. ***Accuracy and valuation*** – financial and other information are disclosed fairly and at appropriate amounts.

Scrutiny of the assertions described above will indicate that some assertions apply to all categories whilst others apply to either two categories or a single category. The following diagram illustrates the breakdown:

ASSERTION	*TRANSACTIONS EVENTS*	*BALANCES assets, liabilities, equity interests*	*PRESENTATION AND DISCLOSURE*
OCCURRENCE	√		√
COMPLETENESS	√	√	√
ACCURACY	√		√
CUT OFF	√		
CLASSIFICATION (and understandability)	√		√
EXISTENCE		√	
RIGHTS AND OBLIGATIONS		√	√
VALUATION AND ALLOCATION		√	√

The auditor's duty is to gather sufficient, appropriate evidence to support the assertion being audited. Whilst every assertion should be considered for audit, the auditor will obviously direct his attention to those assertions which present a risk of material misstatement which, if not detected, could lead the auditor to express an inappropriate opinion on the financial statements (see Chapter 7 for a discussion on audit risk). When the auditor carries out risk assessment procedures for the various account headings, he will consider the risk of material misstatement in terms of the assertions applicable to the account heading. For example he may look at all of the information he has gathered about the company's inventory and then work through the assertions applicable to inventory and its presentation and assess the impact of the information on his assessment of the risk of material misstatement in the inventory account heading. It will be necessary for the auditor to identify the assertions for which evidence should be gathered and then to design an audit plan which will provide enough relevant and reliable evidence on which to base an opinion. Consider the diagram above in conjunction with the following examples:

Example 1

When the auditor gathers evidence about ***sales transactions,*** he will be seeking evidence to support the following assertions:
occurrence - all sales included are genuine sales (not fictitious) of the entity (a genuine sale of the company's goods/services has occurred)
completeness -all sales which were made, have been included in the total of sales made for the year
accuracy – all sales have been recorded appropriately : this implies prices are correct and that the correct discount and VAT rates have been used and correctly calculated.
cut-off – all sales recorded, occurred in the accounting period being audited
classification – all sales have been posted to (recorded in) the proper account. This implies that a credit sale has been posted to the correct debtor's account and that VAT has also been correctly posted.

Take note that the auditor will also ensure that disclosures pertaining to "sales" are ***complete***, ***appropriately classified (understandable),*** and ***accurate***.

The assertions which do not apply to sales are ***existence***, ***valuation*** and ***rights and obligation***. Why is this? It is because these three assertions apply to ***balances*** in the statement of financial position which are carried forward to the following period, and not to ***transactions.*** To explain it slightly differently, the auditor does not try to establish that a sale ***existed*** at reporting date, he seeks evidence that the sale which is included in total sales, actually ***occurred***; furthermore, the auditor does not seek to ***value*** the sale at year end, he seeks to establish that the sale was correctly recorded at the time it was made during the year.

Example 2

When the auditor gathers evidence about plant and equipment he will be seeking evidence to support the following assertions:

completeness - all plant and equipment owned by the company, is included in the balance reflected in the financial statements
existence - all plant and equipment included in the balance, existed at reporting date

valuation and allocation - the plant and equipment has been reflected in the statement of financial position at appropriate amounts; this means that reasonable adjustments have been made for depreciation, impairment and/or obsolescence.
rights - the company has (holds or controls) the right of ownership to the plant and equipment reflected in the statement of financial position (any encumbrances on that ownership must be disclosed).

Take note again that the auditor will address all the assertions pertaining to presentation and disclosure. Presentation and disclosure is far more comprehensive and complex for plant and equipment than for sales (example 1) and obviously presents more risk that there will be material misstatement in the disclosures.

The assertions which do not apply to plant and equipment are ***occurrence*** and ***accuracy, cut-off and classification***. Why is this? It is because these assertions apply only to ***transactions/events*** and not to balances contained in the statement of financial position. The auditor seeks to establish that plant and equipment appearing in the statement of financial position actually ***existed*** at reporting date. Auditing the purchase of the plant and equipment (a transaction) will provide evidence that the purchase ***occurred*** and was correctly recorded (***accuracy***) but it will not provide evidence that the item of plant and equipment was in ***existence*** at year end, (it may have been stolen, sold or destroyed since being purchased), or that it was ***fairly valued*** at year end, (it may have been severely damaged since it was purchased).

In conclusion, once the auditor has gathered sufficient, appropriate evidence relating to the assertions, he will be in a position to evaluate the evidence and express an opinion on the fair presentation of the financial statements.

THE AUDITOR'S TOOLBOX

1. INTRODUCTION

As indicated by ISA 500 – Audit Evidence, audit evidence is obtained by performing
* risk assessment procedures and
* further audit procedures which comprise
  - tests of controls and
  - substantive tests, both tests of detail and analytical procedures.

So what are the procedures for carrying out risk assessment, tests of controls and substantive tests? Are there procedures which apply only to risk assessment? Are tests of controls specific and can any procedure be used as a substantive procedure? The answer is that the seven procedures listed below are the "tools" which the auditor uses to gather evidence and he uses them as he deems fit. Provided the procedure is appropriate to the auditor's objective then it can be used.

For example, ***risk assessment procedures*** might include ***observation*** of the client's manufacturing process to gain an understanding about the client's operations. ***Observation*** may also be used as a ***test of controls***. For example, when employees in the warehouse receive goods from suppliers, they should check the details of the delivery before they sign the supplier's delivery note to acknowledge receipt of the goods. The auditor may ***observe*** this control activity to determine whether they do actually carry it out.

Analytical procedures could be part of ***risk assessment***, for example, the auditor performs an analysis of the company's sales by month, product, branch etc, to gain an understanding of the entity. ***Analytical procedures*** are also used when carrying out ***substantive procedures,*** for example, when considering the valuation of debtors, the auditor might perform a comprehensive comparative analysis of the debtors balance to satisfy himself that the allowance for bad debts is "fair". Analytical procedures are not, however, used as tests of controls, as they do not provide evidence that a control activity is being carried out as it should be.

1.1 ***inspection***: involves examining records or documents, whether internal or external, in paper form, electronic form or other medium, e.g. inspecting a purchase order for an authorizing signature or a physical examination of an asset, e.g. inspecting a piece of equipment for evidence of its existence and condition.

1.2 ***observation***: consists of looking at a process or procedure being performed by others, or of observing the performance of control activities, e.g. observing an inventory count performed by the client's employees.

1.3 ***external confirmation***: involves obtaining a direct written response from a third party to a request/query from the auditor to that third party in paper form or by electronic or other medium, e.g. the auditor requests a client's debtors to confirm the amounts owed to the client at reporting date.

1.4 ***recalculation***: consists of checking manually or electronically, the mathematical accuracy of documents or records.

1.5 ***reperformance***: involves the auditors independent execution of procedures or controls that were originally performed as part of the entity's internal control.

1.6 ***analytical procedures***: involves evaluating financial information through analysis of plausible relationships among both financial and non-financial information.

1.7 ***inquiry***: consists of seeking information, both financial and non-financial from knowledgeable persons within the entity or outside the entity.

As discussed above, it is not possible to categorise each of the above procedures as simply a risk assessment procedure, a test of controls procedure or a substantive procedure. Any of the above procedures (other than analytical procedures as a test of controls), or a combination thereof, can be used when assessing risk or carrying out tests of controls or substantive tests, The procedure will be categorized in terms of what the auditor is trying to achieve.

Example 1.

* ***inquiry – risk assessment***
  The auditor inquires of the head of internal audit as to his assessment of the likelihood of material misstatement of inventory
* ***inquiry – substantive test***
  The auditor makes inquiries of the factory manager as to the impairment writedowns for a particular machine.

Example 2.

* ***reperformance – tests of controls***
  The auditor reperforms the monthly bank reconciliation to confirm that the control activity of reconciling the balance per the cash book and the balance per the bank statement, has been properly carried out. If the reconciliation is incorrect, the control is not working.

* ***reperformance – substantive test***
  The auditor reperforms the year-end bank reconciliation as part of the verification of the bank balance reflected in the year-end financial statements (same procedure, different objective!).

Example 3.

* ***inspection – risk assessment***
  The auditor examines the minutes of meetings of directors to identify important decisions which have been taken, which may affect the financial statements.
* ***inspection – tests of controls***
  The auditor inspects a sample of purchase orders over R500 000 for the authorizing signature of the senior purchase officer to confirm that the control over authorizing purchases in excess of this amount, is being exercised. All purchases over R500 000 must be authorized by the senior purchase officer.

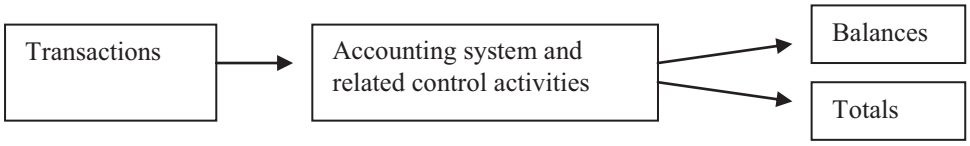
* ***inspection – substantive test***
  The auditor inspects a letter from a financial institution confirming the amount, and terms of a loan made to the client company.

Example 4.

* ***observation – risk assessment***
  The auditor observes the operation of the production line in a manufacturing company as part of assessing the risk of material misstatement in the valuation of work in progress (possibly to decide whether it will be necessary to engage an expert).
* ***observation – tests of controls***
  The auditor observes the procedures actually conducted by warehouse personnel when receiving goods ordered.

2. WHY PERFORM TESTS OF CONTROLS?

2.1 The diagram below is a simple representation of the flow of transactions through an accounting system:



For example, when credit purchase transactions are processed through the accounting system the trade creditors balance is increased as is the total on the purchases account. When creditors are paid, the payment transactions are processed through the accounting system and the trade creditors balance is decreased. The total of purchases remains unaffected but the cash (bank) account balance is reduced. When wage transactions are processed through the accounting system, the balance on the cash (bank) account is reduced and the wage expense total increased. Remember, as the transactions are recorded on source documents and passed through the accounting system, they will be subjected to a range of control activities. The conclusion that can be drawn is that if the accounting system and related control activities are sound, the balances and totals produced will be sound. The auditor who is interested in the fair presentation of balances and totals, could therefore test the accounting system and related control activities to determine whether they produce reliable balances and totals. These tests are known as ***tests of controls***.

2.2 ISA 315 (revised) requires that the auditor, as part of his identifying and assessing risk, obtains an understanding of the client's internal control. An understanding of internal control assists the auditor in identifying types of potential misstatements and factors that affect the risks of material misstatement. If the auditor concludes that the internal control system, based on his understanding, is sound, he will build tests of controls into his audit plan to satisfy himself of the ***operating effectiveness*** of the controls. In other words, his understanding of the internal control system created an ***expectation*** that the controls are operating effectively and now, as a further audit procedure he must test the controls to see if they are actually working.

If the tests of controls provide sufficient appropriate evidence that the controls are operating effectively, the auditor will be more confident that the balances and totals produced by the system are valid, accurate and complete, and hence he will need to spend less time on conducting substantive tests.

2.3 Is it acceptable for the ″further audit procedures″ to consist only of tests of controls? The answer is no! Even if the auditor finds that the accounting system and related control activities are excellent and operating effectively, he must realise that

* all internal control systems have inherent limitations which make them less than 100% efficient (see page 5/4 under Internal Control)
* the internal control system may have been operating effectively at the time the auditor performed his tests but this does not mean it did so throughout the year
* there will still be inherent risk at both financial statement level and at assertion level to consider (see Chapter 7)

* there is a large amount of information in a set of financial statements, which is not generated through the internal control system and which the auditor will still need to substantiate.

Successful tests of controls will reduce the extent, and possibly, change the nature of substantive tests, but cannot eliminate the need to perform substantive tests.

3. WHY PERFORM SUBSTANTIVE PROCEDURES?

3.1 The auditor's objective is to be in a position to express an opinion on whether fair presentation has been achieved in the annual financial statements. Financial statements consist of a collection of balances (in the statement of financial position) and a summary of totals (the statement of comprehensive income), and accompanying notes. As discussed above, tests of controls on their own cannot provide the auditor with sufficient, appropriate evidence pertaining to these balances, totals and disclosures and it will therefore be necessary for the auditor to perform procedures of a substantive nature.

3.2 Substantive procedures may be performed on balances and totals themselves or on the individual transactions making up the balance or total and on disclosures. They may be broadly distinguished as ***tests of detail*** or ***analytical procedures***. When conducting tests of detail the auditor carries out procedures on the specific detail of a transaction, account balance or disclosure.

He may inspect the date on a sample of purchase invoices to confirm that the purchase was recorded in the correct accounting period or confirm the cost at which a specific item of equipment was raised in the accounting records against the purchase invoice and payment records for that item, or he may confirm the details of a contingent liability disclosed in the notes by inquiry of the financial director and inspection of correspondence from the client's attorneys.

When conducting analytical procedures the auditor does not look at the detail of specific transactions, balances or disclosures but rather attempts to evaluate financial information through analysis of plausible relationships among both financial and non-financial data, for example, comparison of sales, month to month, year to year, by product, by region, to determine whether sales for the current period are ″plausible″ or as expected when compared to other periods. If there are fluctuations or inconsistencies, the auditor will attempt to establish the reason. These analytical procedures might provide the auditor with a general idea as to whether sales have been overstated (occurrence assertion) and whether accounts receivable have been overstated (existence assertion).

3.3 Substantive procedures seek to provide evidence to support the financial statement assertions. When performing substantive tests the auditor is interested in the following assertions:

* ***balances*** – completeness, existence, valuation, rights and obligation, presentation and disclosure.
* ***transactions*** – completeness (totals), occurrence, accuracy, cut-off, classification and, presentation and disclosure.
* ***disclosures*** – occurrence and rights and obligations, completeness, classification and understandability, accuracy and valuation.

4. VOUCHING AND VERIFYING

Vouching and verifying are terms commonly used by auditors; ***vouching*** relates to the audit of ***transactions***, and ***verifying*** relates to balances. Both terms signify a "collection" of different substantive procedures. For example, to ***vouch*** a sales transaction the auditor will, inter alia, ***inspect*** documentation, may ***enquire*** about discounts and may check the arithmetical accuracy of the invoice ***by recalculation***. To ***verify*** the debtors balance the auditor may, inter alia, obtain written ***confirmation*** from the debtors and may make ***enquiries*** as to how the allowance for bad debts was calculated and then ***reperform*** the aging of debtors.

AUDIT SAMPLING

1. PRINCIPLES OF SAMPLING

It is seldom that an auditor can examine every item in a population e.g. all sales invoices or every inventory item, and although this is a limitation of the audit function, it is generally understood that it is a limitation that will always remain. There are populations where all "items" in that population are audited – for example, all loans to directors will normally be subject to audit, and all minutes of shareholders meetings will be inspected, but in general populations are far too large to audit every item. To do so would not be time or resource efficient.

ISA 530 – Audit Sampling requires that when designing audit procedures, the auditor should determine appropriate means for selecting items for testing so as to gather sufficient, appropriate audit evidence to be able to draw reasonable conclusions on which to base the auditor's opinion. The statement deals with the auditor's use of statistical and non-statistical sampling when designing and selecting the audit sample, performing tests of controls and tests of detail, and evaluating the results from the sample.

It must also be born in mind that the results obtained from auditing a sample of items, will not be the only evidence gathered about the population being audited. Evidence gained from other audit procedures, such as analytical procedures, will corroborate the evidence gained from the sampling procedures. The audit is much like a jigsaw puzzle with numerous pieces of evidence combining to provide the complete picture.

An important aspect of sampling is that the results of the tests on the sample must be extrapolated over the population as a whole. The auditor must form an opinion on the population; it is therefore of little use to draw the conclusion that "we only found three errors in the sample, so there is no problem." The question to ask is "how many errors are there in the entire population?" The methods of extrapolating the sample results over the population will vary depending on whether statistical or non-statistical sampling has been carried out. Where statistical sampling has been used, the extrapolation will be more defendable than where the auditor has used some judgmental process to extrapolate.

2. DEFINITIONS

ISA 530 –Audit Sampling provides the following definitions

Audit sampling – involves the application of audit procedures to less than 100% of the items within a population of audit relevance such that all sampling units have a chance of selection in order to provide the auditor with a reasonable basis on which to draw conclusions about the entire population.

Anomaly – a misstatement or deviation that is demonstrably not representative of misstatements or deviations in the population.

Population – means the entire set of data from which a sample is selected and about which the auditor wishes to draw conclusions. For example, all items included in an account balance or a class of transactions are populations. A population may be divided into strata, or sub-populations, with each stratum being examined separately.

Sampling risk – the risk that the auditor's conclusion based on a sample may be different from the conclusion that would be reached if the entire population were subjected to the same audit procedure. There are two types of sampling risk:

* the risk that the auditor will conclude, in the case of a test of controls that controls are more effective than they actually are, or in the case of tests of detail, that a material misstatement does not exist when in fact it does. The auditor is primarily concerned with this type of erroneous conclusion because it affects audit ***effectiveness*** and is more likely to lead to an inappropriate audit opinion

* the risk that the auditor will conclude, in the case of a test of controls, that controls are less effective than they actually are, or in the case of a tests of detail, that a material misstatement exists when in fact is does not does not. This type of erroneous conclusion affects audit

efficiency because it will usually lead to additional audit work being carried out to establish that the initial conclusion were incorrect.

Non-sampling risk - is the risk that the auditor arrives at, an erroneous conclusion for any reason not related to sampling risk, e.g. because he has applied his sampling plan incorrectly, adopted an inappropriate procedure or misunderstood the results of his sampling exercise.

Sampling unit - means the individual items constituting a population, for example, credit entries on bank statements, sales invoices listed in the sales journal, inventory line items, or individual debtors balances in the debtors ledger.

Statistical sampling - means any approach to sampling that has the following characteristics:

* random selection of a sample; ***and***
* use of probability theory to evaluate sample results, including measurement of sampling risk.

A sampling approach that does not have these characteristics, is considered non-statistical sampling.

Stratification - is the process of dividing a population into sub-populations, each of which is a group of sampling units which have similar characteristics (often monetary value) e.g. debtors balances from R1 to R10 000, R10 001 to R25 000, R25 001 to R50 000.

Tolerable rate of deviation – a number or percentage of deviations from prescribed internal control procedures set by the auditor in respect of which the auditor seeks to obtain an appropriate level of assurance that the number/percentage set by the auditor is not exceeded by actual deviations in the population.

Tolerable misstatement - a monetary amount set by the auditor in respect of which the auditor seeks to obtain an appropriate level of assurance that the monetary amount set by the auditor is not exceeded by the actual misstatement in the population.

3. TESTS OF CONTROLS AND SAMPLING

Having obtained an understanding of the accounting and internal control systems, the auditor will be in a position to identify the characteristics or attributes which indicate the performance of a control procedure, for example, the signature of the credit controller on a customer order indicating credit approval. Once the indicators have been identified, the auditor can test the control by extracting a sample from the entire population of customer orders and inspecting the authorising signature.

The auditor should be quite clear about what evidence is provided by the test. For example, this test will only provide evidence of orders which did not contain the credit controller's signature and therefore may have been processed without the approval of the credit controller. The test will, however, ***not*** indicate whether the credit controller actually considered the creditworthiness of the customer before approving the order. Whether the credit controller is actually performing the control procedure will probably be best established by investigating whether the customer subsequently paid, and that payment was made on time.

4. SUBSTANTIVE PROCEDURES AND SAMPLING

Substantive procedures are concerned with balances and amounts. Sampling may be used to gather evidence about one or more assertions relating to the balance or amount, or to make an independent estimate (projection) of some amount. For example, a sample of debtors may be selected for positive verification to obtain evidence about the existence of debtors, or, using an appropriate sampling plan, the total value of inventory, based upon a sample selected, may be projected for comparison with the value represented by the directors in the financial statements.

5. STATISTICAL VERSUS NON-STATISTICAL APPROACHES

The decision as to whether to use statistical or non-statistical sampling is a matter of professional judgement. Statistical sampling and non-statistical sampling are not mutually exclusive, certain aspects of statistical sampling may be used when performing a non-statistical sample. For example, the sample size

may be decided upon on a judgmental basis (non-statistical) but the items to be selected may be chosen using computer generated random numbers (statistical approach). The important point is however, that valid statistically based evaluation of the sampling results can only take place where all the characteristics of statistical sampling have been adopted, e.g. sample size, selection of items, extrapolation, evaluation, are properly applied in terms of probability theory.

6. STEPS IN THE SAMPLING EXERCISE

An important consideration in undertaking a sampling exercise is whether it will be statistically or non-statistically based. The decision will be one of professional judgement, but will be based on the level of assurance required by the auditor, the skills and time available, and the "defensibility" of the results which the auditor might require. Regardless of this decision the steps to be taken remain broadly the same.

6.1 Determine the objectives of the procedure

For example, the auditor may wish to establish:

* that for every entry in the purchase journal, there is a signed goods received note (test of controls), or
* that the individual debtor's balances in the debtors ledger pertain to debtors who exist (substantive).

6.2 Determine the procedure to be performed

* This includes specifying clearly the ***error (deviation or misstatement) condition***. So in the first example given in 6.1 above, the procedure will be to select a sample of entries in the purchase journal (note direction of test) and trace to the purchase invoice and see whether it has a signed GRN attached. The deviation is the absence of a GRN (usually the presence of a GRN without a signature will be tested separately).
* In the second example in 6.1 above, the procedure may be to select debtors' balances for positive circularisation. The misstatement will be the inclusion in the client's debtors ledger of any debtor who does not exist.

6.3 Confirm that the population is appropriate and complete

* This is the population from which the sample is to be selected ***and the population upon which an audit conclusion is to be made***.
* In the examples in 6.1 the population will be ***all*** purchase journal entries and ***all*** debtors balances as per the debtors ledger.
* A very important consideration is that ***all*** units in the population must be available for selection. In the examples used thus far, ensuring that all units in the population are considered for selection will be relatively easy. The problem that arises with regard to completeness of the population usually occurs where the unit of sample is a document. Here extensive checks on sequence and stationery control are necessary to be sure that all sequences of documents used during the year, are included.

6.4 Define the units of the population

In the examples in 6.1, the units would be entries in the purchase journal (a numbering system identifying each entry would have to be developed to implement the sampling plan), and each debtor in the general ledger. Note that the units of the population, which are selected for the sample, become the units of the sample.

6.5 Determine the sample size

The overriding requirement for determining the sample size is whether the sampling risk will be reduced to an acceptably low level. For example, if you have a population of 10 000 items and you select a sample of only 15 items, sampling risk would be very high – so the question arises, "How many of the items should be selected for the sample to reduce sampling risk to an acceptable level?"

Whether statistical or non-statistical approaches are to be used, professional judgement will still play a large role. With non-statistical approaches, the sample size is virtually entirely based on professional judgment. With statistical approaches, the auditor is forced into making judgements about specific matters which are then applied to a formula or table which will give the sample size. These specific judgments are described as follows:

* ***confidence level***: confidence indicates, as a percentage, how often a sample will correctly represent the population. The auditor must decide how "confident" he wants to be about his conclusions. The more confident he wishes to be, the larger the sample needs to be. Remember that the auditor must draw his conclusion (form an opinion) on the population, and therefore wants the sample to be representative of the population.
In the first example from 6.1, a 90% confidence level would mean statistically that if 100 random samples were selected, 90 of them would be expected to give a reliable representation of the extent to which purchase journal entries are supported by GRNs, and 10 ***may not***.

* ***tolerable misstatement/tolerable rate of deviation:*** this is the maximum extent of "error" that the auditor is willing to accept and still feel that the objective of the sampling procedure has been achieved. The converse of this is the extent of misstatement or rate of deviation which the auditor decides is unacceptable (which will lead to more extensive, or alternative procedures). In the first 6.1 example, if the auditor wishes to rely on a GRN supporting purchase journal entries (i.e. goods were received) he or she must be sure that it happens in, say, 97% of cases. The tolerable deviation will then be 3%. In the debtors example, the tolerable misstatement would be expressed in rands e.g. R10 000 of the balance pertains perhaps to debtors for which the auditor cannot prove existence using the positive circularization procedure. The less deviation or misstatement the auditor is prepared to tolerate, the larger the sample size.

* ***expected misstatement/rate of deviation:*** most sampling plans require an estimate of the expected "error rate" to be made because the greater the anticipated misstatement/rate of deviation, the larger the sample size will be in order to achieve sufficient assurance. The estimate is based either on past experience, knowledge of the business or a pilot sample.

* ***the population size (the number of sampling units):*** some sampling plans require that the population size be known to be able to arrive at the sample size. Other sampling plans do not. In our example, the population will be every entry in the purchase journal, or every debtor in the debtors ledger. For very large populations, variation in the size of the population has little, if any, effect on sample size.

6.6 Select the sample

Having calculated the sample size as above, the decision has to be taken as to ***how*** to select these items. The following methods are suggested:

* ***random****:* Every unit must have an equal chance of selection and the selection can be made manually by using random number tables, or by computer using random number generation software.

* ***systematic:*** This involves selecting a random starting point and then selecting every, say, 30th item. As there may be patterns within the population this is a risky, though cost effective, method.

* ***haphazard:*** Here the auditor attempts to simulate randomness by avoiding conscious bias or predictability and not following a structured technique. In a ***non***-statistical sample it is an acceptable technique. It is ***not*** a valid method of selection if using statistical sampling as guaranteed randomness is a prerequisite of the statistical sampling approach.

* ***block***: This involves selection of a block of contiguous (e.g. numerically consecutive) items from within the population. (This is not often an appropriate selection technique where the auditor wishes to draw valid inferences about the entire population).

* ***monetary unit sampling*** is a value weighted selection method in which the sampling unit is every rand in the population. Every n^{th} rand is then selected. This will result in larger amounts being selected because larger amounts have more rand units. For example, if we are selecting a sample of debtors from the debtor's list, we do not consider the individual debtors to be the sampling unit, we regard each rand in each balance to be the sampling unit. Therefore we select every n^{th} rand, the chances are greater that the n^{th} rands will be contained in large balances than in small balances. The debtors balances into which the n^{th} rands fall, will be selected for the sample.

6.7 Perform the audit procedures

As determined in (6.2) above.

6.8 Analyse the nature and cause of deviations and misstatements

The auditor should analyse the sample results and consider the nature and cause of deviations and misstatements identified. This is done to provide the auditor with more insight into the "errors" which in turn, may provide evidence that further procedures are necessary, or that risk should be reassessed. Two examples will illustrate the importance of this procedure.

Example 1: When performing tests of controls, the analysis of deviations discovered in the sample indicates the presence of management override. This may suggest to the auditor that fraudulent activity is taking place. In turn this may lead to a reassessment of all information supplied by management and the extention of testing to other areas of the audit.

Example 2: On analysis the auditor establishes that certain "errors" in the sample arose out of an isolated or unique event. (This is defined as an anomaly). This could occur, for example, where the errors can be tied back to a temporary staff member who had made the "errors" whilst standing in for the permanent staff member for a short period during the year. If this unique situation is projected over the population, the result will be very misleading and may result in the performance of unnecessary procedures. (The extrapolation of the sample results must be conducted once the anomalies have been removed from the sample results.)

6.9 Project the sample results over the population

At this point the auditor will calculate the actual number of misstatement/deviations (as defined) in the ***sample***. Where statistical sampling is used, the auditor will arrive at the misstatement/deviation rate for the population by applying the various determinants to the relevant ***formula or table***.

Where a non-statistical approach is used, some other method of projecting the sample over the population must be applied, e.g. proportion. Although many firms do this, its validity is questionable.

6.10 Evaluate

Once the sample result is projected over the population, it is compared to the tolerable deviation/misstatement. The auditor then concludes on the sample in terms of his confidence level and precision if these have been set. Should the results of a sampling exercise be unsatisfactory, the auditor may:

* request management to investigate the deviations/misstatements and the potential for further deviations/misstatements, and to make any necessary adjustments; and/or
* modify planned audit procedures. For example, in the case of a test of controls, the auditor might extend the sample size, test an alternative control or modify related substantive procedures.

7. CONCLUSION

Sampling is an integral part of auditing. Although it has its limitations in the audit context, it is used extensively on virtually every audit. Both statistical and non-statistical approaches are used and both have their place. Evidence obtained from sampling is not in itself complete and is persuasive rather than conclusive. However, it is an important component in the process of gathering sufficient, appropriate evidence.

CHAPTER 6

AN OVERVIEW OF THE AUDIT PROCESS

INTRODUCTION 6/2

QUALITY CONTROL FOR THE AUDIT OF FINANCIAL STATEMENTS 6/2

1. Leadership responsibilities 6/2
2. Ethical requirements 6/2
3. Independence 6/3
4. Acceptance and continuance of client relationships 6/3
5. Assignment of engagement teams 6/3
6. Engagement performance 6/4
7. Consultation and differences of opinion 6/5
8. Engagement quality control review 6/5
9. Monitoring 6/5

THE AUDIT PROCESS

1. Diagrammatic representation of the audit process and supporting narrative description 6/6
2. The role of the International Standards on Auditing (ISAs) in the audit process 6/8

PRELIMINARY ENGAGEMENT ACTIVITIES 6/9

1. Pre-conditions for an audit 6/9
2. Prospective clients and continuance with an existing client 6/9
3. Compliance with standards 6/9
4. Procedures to gather "preliminary engagement" information 6/10
5. Establishing an understanding of the terms of the engagement 6/11

PLANNING 6/13

1. Introduction 6/13
2. The overall audit strategy 6/13
3. The audit plan itself 6/15
4. Materiality 6/15
5. Planning and conducting risk assessment procedures 6/15
6. Planning further audit procedures based on the risk assessment 6/17

RESPONDING TO ASSESSED RISK 6/20

1. Overall response at financial statement level 6/20
2. Audit procedures to respond to the assessed risk of material misstatement at the assertion level (further procedures) 6/20
3. Audit procedures carried out to satisfy the requirements of the ISAs (other procedures) 6/21

EVALUATING, CONCLUDING AND REPORTING 6/21

1. Sufficient, appropriate evidence 6/22
2. Uncorrected misstatements 6/22
3. Applicable financial reporting standards 6/23
4. Events occurring after the reporting date 6/23

INTRODUCTION

This chapter and chapter 7 – Important elements of the audit process, are interrelated and should be studied in conjunction with each other to obtain a solid understanding of the audit process.

Chapter 6 provides an overview of the audit process, and includes a reasonably comprehensive coverage of some stages (or aspects of a stage) of the process, e.g. preliminary engagement activities, whilst chapter 7 provides a detailed discussion on the important elements of the audit process, e.g. materiality. This is not to suggest that those aspects covered in chapter 6 are not important, but rather that the elements covered in chapter 7 require more detailed explanation.

Once you have an idea of what is involved overall, you will better understand how the detail fits in. Remember that the auditor's objective is to be in a position to form an opinion on whether the financial statements fairly present, in all material respects, the financial position of the company at a particular point in time, and the results of its operations for a period which ended at that point in time. The auditor goes through a process to achieve this objective.

However, before considering the overview of the audit process it is necessary to gain an understanding of ISA 220 which deals with quality control for an audit of financial statements. It is of utmost importance that all stages of the process are carried out with a high level of competence and compliance with the standards which are expected of a "professional" accountant. To ensure that this happens, audit firms are required to put in place policies and procedures to ensure that the desired quality standards are achieved for all aspects of the audit. Quality control is not only motivated by a need and desire to offer a highly professional and meaningful service but the most effective safeguard for the auditor against the risk of being sued for negligence by a client is to perform quality audits. Two statements are relevant here ISA 220, and ISQC1 – Quality Control for Firms that perform Audits and Reviews of Historical Financial Information, and other Assurance and Related Services Engagements.

ISA 220 is summarised below; reference can be made to ISQC1 for expanded explanations. ISA 220 seeks to provide guidance on the specific responsibilities of firm personnel regarding quality control procedures for audits. In effect the statement places a collective responsibility on the ***engagement team*** to conduct a quality audit within the context of the firm's system of quality control. Every team needs a captain to take charge, and in terms of ISA 220 the ***engagement partner*** fulfils this role.

QUALITY CONTROL FOR THE AUDIT OF FINANCIAL STATEMENTS – ISA 220

1. LEADERSHIP RESPONSIBILITIES FOR QUALITY ON AUDITS

The engagement partner (designated auditor – Auditing Profession Act) is required to take responsibility for the audit engagement. The tone of the audit should be set by the engagement partner, who by his actions and by direct communication with his team, should emphasize the importance of

1.1 performing work which complies with professional standards and regulatory and legal requirements and complies with the firm's quality control policies and procedures.

1.2 issuing auditor's reports that are appropriate.

1.3 the engagement team's ability to raise concerns without fear of reprisal.

1.4 the element of ***quality*** in all aspects of the audit.

2. ETHICAL REQUIREMENTS

An essential requirement for achieving quality on the audit is that the engagement team apply the highest level of professional ethics. The fundamental principles of which include:

* integrity (self honesty)
* objectivity (independent thought, freedom from bias)
* professional competence and due care
* confidentiality and
* professional behaviour

Although it is the responsibility of the firm to recruit employees who display and believe in these fundamental principles, it is the responsibility of the engagement partner to encourage and develop ethical behaviour on the audit. Equally important is the partner's duty to be alert to evidence of non-compliance by the engagement team. Any such evidence should be followed up, dealt with, and the outcome documented.

3. INDEPENDENCE

ISA 220 underlines the importance of independence (as part of objectivity) in respect of audit engagements by dealing with it separately. The statement requires that the engagement partner ***"forms a conclusion on compliance with independence requirements that apply to the engagement"***. A clear duty is placed on the engagement partner to

3.1 obtain relevant information from the firm to identify and evaluate circumstances and relationships that create threats to independence e.g. the proposed manager of the audit team is married to the client's financial controller.

3.2 evaluate any potential breaches to determine whether they present a threat to the firm's independence which is ***not*** clearly insignificant. In the example in 3.1, the threat would be significant.

3.3 take appropriate action to eliminate or reduce the threat to an acceptable level. In the example in 3.1, the appropriate action would be to leave the proposed manager off the engagement team.

3.4 document conclusions on the independence of the audit team.

4. ACCEPTANCE AND CONTINUANCE OF CLIENT RELATIONSHIPS

It is the duty of the audit firm to have quality control procedures in place regarding the acceptance and retention of clients e.g. there should be procedures to determine whether the directors of a potential audit client have integrity. This duty is extended to the engagement partner who is required on an ongoing basis to evaluate

4.1 the integrity of the principle owners, key management and those charged with governance of the entity.

4.2 whether the engagement team is competent to perform the audit and has the necessary time and resources.

4.3 whether the firm and engagement team can comply with the ethical requirements.

If the engagement partner obtains information that would have caused the firm to decline the audit engagement had it had access to the information prior to accepting the engagement, the engagement partner should convey the information to the firm so that appropriate action can be taken. The firm may have been seriously misled by the directors as to the activities/operations of the company, a situation which is only discovered once the audit is underway. For example, the company is involved in frequent and regular illegal acts ranging from foreign exchange contraventions and illegal import of counterfeit goods. In this instance the auditor would be required to meet its Sec 45 Auditing Professional Act 2005 – Reportable Irregularities duty, and would ultimately withdraw from the engagement.

5. ASSIGNMENT OF ENGAGEMENT TEAMS

The engagement partner should be satisfied that the engagement team (collectively and including experts who are not employees of the firm) has the appropriate ***capabilities, competence*** and ***time*** to perform an audit of the appropriate quality. The appropriate capabilities and competence include the following

5.1 an understanding of, and practical experience with, audit engagements of a similar nature and complexity.

5.2 an understanding of professional standards and regulatory and legal requirements.

5.3 appropriate technical knowledge, including knowledge of relevant information technology and specialized areas of accounting or auditing e.g. how to account for and audit financial derivatives.

5.4 knowledge of relevant industries in which the client operates.

5.5 ability to apply professional judgement (and an appropriate level of professional skepticism).

5.6 an understanding of the firm's quality control policies and procedures.

6. ENGAGEMENT PERFORMANCE

The engagement partner is required to take responsibility for the direction, supervision and performance of the audit and a review of the audit performance. His objective is to ensure that the audit has been carried out in compliance with professional standards, regulatory and legal requirements, and that sufficient appropriate audit evidence has been obtained to support the conclusions reached and the audit opinion to be given, i.e. the auditor's report being appropriate in the circumstances.

6.1 Direction

The engagement partner directs the audit engagement by informing the members of the engagement team of

* their responsibilities (e.g. maintaining objectivity, adopting a suitable level of professional skepticism, ethics etc)
* the nature of the entity's business
* the objectives of the work to be performed
* risk-related issues and potential problems
* the detailed audit strategy and audit plan.

6.2 Supervision

This includes the following

* monitoring progress on the audit
* considering the capabilities and competence of the individual members of the team, whether they have the necessary time, whether they understand their instructions and are carrying them out in accordance with the audit strategy and plan
* addressing significant issues which arise on audit, and modifying the audit strategy and audit plan appropriately
* identifying matters for consultation or consideration by more experienced members of the engagement team.

6.3 Review

Review procedures are conducted on the basis that more experienced team members, including the engagement partner, review the work performed by less experienced team members. A reviewer will consider whether

* the work has been performed in accordance with professional standards and regulatory and legal requirements
* significant matters have been raised for further consideration
* appropriate consultations have taken place (and recommendations implemented and documented)
* there is a need to revise the nature, timing and extent of audit work
* the work performed supports the conclusions reached and is adequately documented
* the evidence obtained is sufficient and appropriate to support the auditor's report
* the objectives of the audit procedures have been achieved.

Note: The engagement partner, in addition to his overall responsibility for the review process must also carry out timely reviews of specific matters such as

* critical areas of judgement applied on the audit
* significant risks and responses thereto.

7. CONSULTATION AND DIFFERENCES OF OPINION

Difficult or contentious issues frequently arise on audit. It is the responsibility of the engagement partner to ensure that where such issues arise, they are resolved by consultation with appropriate persons either within the firm or external to it. The engagement partner should ensure that the nature, scope and conclusions resulting from consultations are ***documented, confirmed*** with the consultant and ***implemented***.

Where differences of opinion arise out of difficult or contentious issues, the firm's policies and procedures for settling the difference should be followed e.g. engagement of additional experts, arbitration by a senior partner from another office of the firm.

8. ENGAGEMENT QUALITY CONTROL REVIEW

An important requirement of ISA 220 is that for audits of listed entities (but not restricted to listed companies), the firm should appoint an engagement quality control reviewer to conduct a quality control review of the engagement ***as a whole*** before dating the auditor's report.

8.1 Qualifications and objectives

A partner, or other person in the firm, or a suitable external person (or a team of such persons) with sufficient and appropriate experience and authority to objectively review

* the significant judgements made by the engagement team and
* the conclusions reached in formulating the auditor's report.

8.2 Matters to be considered by the reviewer

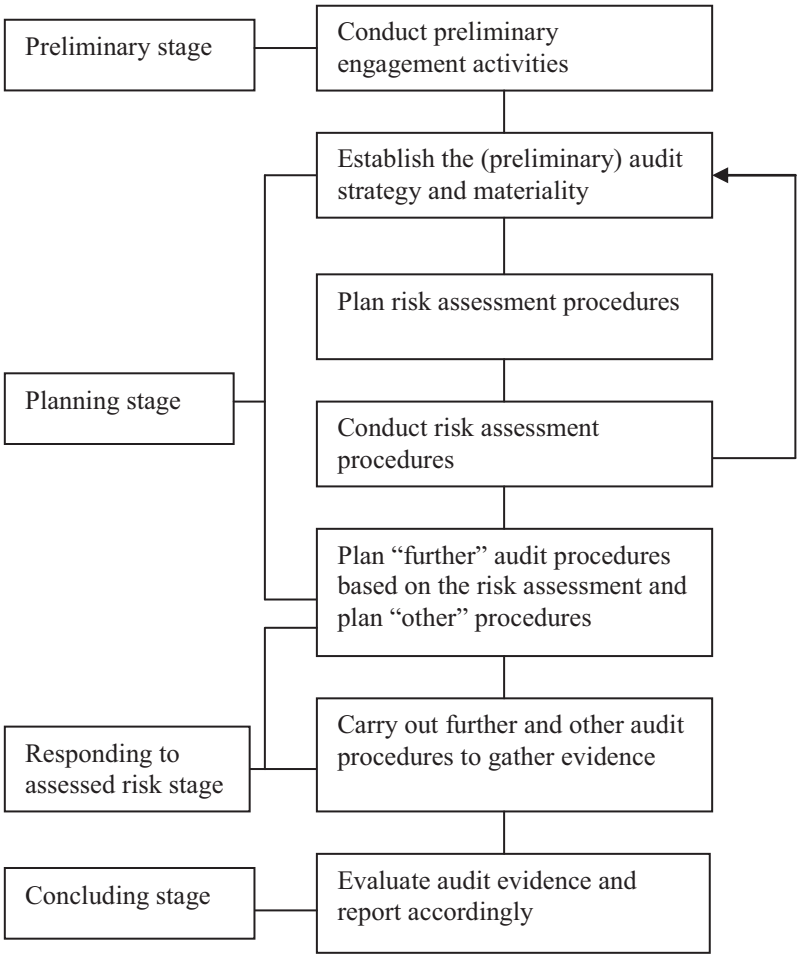
* the independence of the audit team
* the identification of risk and the team's responses thereto (including the risk of fraud)
* judgements made in respect of materiality and significant risks
* the outcome of consultations in respect of contentious or difficult audit issues, and the conclusions arising from these consultations
* the significance and treatment of corrected and uncorrected misstatements identified on the audit
* issues to be communicated to management and those charged with governance, other parties (e.g. IRBA)
* whether audit documentation reflects the work performed and supports the conclusions reached
* the appropriateness of the auditor's report to be issued.

9. MONITORING

Audit firms are required to monitor their quality control procedures to ensure that they are relevant, adequate, operating effectively and complied with in practice.

THE AUDIT PROCESS

1. DIAGRAMMATIC REPRESENTATION OF THE AUDIT PROCESS



Note: This diagram should only be used to obtain an overview of the audit process. The stages of the audit are not "stand alone units" and the activities within each stage do not always fit neatly into the order presented. The different aspects or activities within planning are far more interrelated and dependent on each other, than is reflected in the diagram and the order in which they occur is not as clear cut.

For example, the audit strategy may change once risk assessment procedures have been carried out. Risk assessment procedures cannot be planned until a materiality level has been set but the materiality level may also change once the risk assessment procedures have been carried out, or even as they are being carried out.

Even when carrying out planned procedures, the auditor might decide to change the plan to respond to new information. Neither the audit strategy nor the audit plan is static; they will change as the audit unfolds.

The above chart and brief narrative for each stage below should provide you with a basic understanding of the audit process; the more detailed discussions which follow in the rest of chapter 6 and in chapter 7 will then be placed in context.

1.1 Preliminary stage

This stage consists of what are termed preliminary engagement activities which take place before an audit engagement is accepted. This includes:

* establishing whether the pre-conditions for an audit are present
* performing procedures to determine whether the audit firm wishes to establish (in the case of a prospective client), or continue (in the case of an existing client) the client relationship
* establishing whether the client can be appropriately serviced, i.e. can the auditor do the audit properly?
* evaluating whether the firm is able to comply with the ethical requirements relating to the engagement, e.g. is there a threat to independence?
* establishing an understanding of the terms of the engagement including confirming that there is a common understanding between the auditor and management, and those charged with governance, of the terms of the audit engagement.

1.2 Planning stage

As you can see from the diagram, this stage has a number of activities within the stage itself. They are:

* establishing the audit strategy – this will be a preliminary idea of what the scope, timing and direction (focus) of the audit will be and what resources (skills, number of staff, etc) will be needed on the audit
* considering materiality – this entails the auditor making a judgement about the size of misstatements which will be considered material
* planning risk assessment procedures – this entails planning the procedures which will be conducted to obtain an understanding of the entity and its environment so that the identification and assessment of the risk of material misstatement can take place.
* conducting risk assessment procedures – this entails carrying out the planned risk assessment procedures and identifying and assessing the risk of material misstatement as they progress
* planning "further" and "other" audit procedures – this amounts to planning the "further" procedures which will be conducted to address the identified risks, in such a manner that audit risk (the risk of giving an inappropriate opinion) is reduced to an acceptable level, and planning "other" procedures necessary to satisfy the requirements of the ISAs (this is explained below).

Note (a): The auditor in effect develops ***two*** audit plans, or perhaps, to be more correct, one audit plan with two sections. Either way:

* ***plan 1*** will describe the nature, timing and extent of procedures to ***identify and assess risk***
* ***plan 2*** will describe the nature, timing and extent of ***further audit procedures*** which are needed to respond to the risks identified at assertion level ***and***
* ***plan 2*** will also describe ***other audit procedures*** which must be carried out to ensure that the audit complies with the ISAs. To illustrate, if part of our audit strategy is to make use of internal auditors, we must plan procedures to comply with ISA 610 (Revised) – Using the work of Internal Auditors. For example, we must carry out procedures to evaluate the internal auditors before we can rely on them. These will not be "further procedures" ***directly*** related to the risk assessment but rather procedures arising from our duty to comply with the ISAs.

Note (b): Making the distinction between "further" and "other" procedures is not particularly important, getting the overall response right and conducting the procedures properly is far more important.

Note (c): The audit strategy will be affected by the identification and assessment of risk. As indicated earlier, the audit strategy is initially based on preliminary knowledge about the audit and the client. When identifying and assessing risk, the audit team will discover information which may change the audit strategy. Neither the strategy nor the plan are static; they will change as the audit unfolds.

Note (d): Obviously it is impossible to develop an effective audit plan for ***further*** audit procedures and ***other*** procedures before the risk assessment procedures have been carried out, so for purposes

of simplifying the audit process, we will regard the identification and assessment of the risk of material misstatement as part of the planning stage.

Note (e): The setting of materiality guidelines, which are the auditor's judgements about the size of misstatements that will be considered material, must be carried out before risk assessment procedures take place but may also change as the audit unfolds.

1.3 Responding to assessed risk stage

ISA 330 – The auditor's responses to assessed risk, states that the auditor should obtain sufficient, appropriate audit evidence regarding the assessed risks of material misstatement through designing and implementing appropriate responses to those risks. The auditor's first "response" to assessed risk is to ***plan*** "further" and "other" audit procedures (so this response has been linked to planning in the diagram) and thereafter to

* respond in a general sense to assessed risk at ***financial statement level***, e.g. assigning appropriately experienced and skilled individuals to the audit team to execute the plan
* respond specifically to assessed risk at ***assertion level*** by ***carrying out*** tests of controls and substantive tests so as to gather sufficient, appropriate evidence that material misstatement has not gone undetected and
* ***carry out*** those "other" procedures which are required to comply with the ISAs. Again these are not clearly defined "stand alone" steps; they combine with and influence each other.

1.4 Concluding stage

This stage of the process consists of:

* evaluating and concluding on the audit evidence gathered – this means evaluating all the audit evidence gathered to determine whether it is sufficient (enough) and appropriate (relevant and reliable) to draw a conclusion of fair presentation
* formulating the audit opinion and drafting the audit report which conveys that opinion.

2. THE ROLE OF THE INTERNATIONAL STANDARDS ON AUDITING (ISAs) IN THE AUDIT PROCESS

South Africa has adopted the IFAC auditing standards (ISAs). The standards provide guidance on how the audit process is to be conducted. The statements in which the standards are documented, do not contain detailed lists of procedures. They stipulate an objective and provide explanatory comment on how the standard should be achieved. There are standards which are directly applicable to each stage of the audit, for example (this list is by no means exhaustive):

Preliminary stage	ISA 210 – Agreeing the terms of audit engagements
	ISA 220 – Quality control for an audit of financial statements
Planning stage	ISA 300 – Planning an audit of financial statements
	ISA 315 (Revised) – Identifying and assessing the risks of material misstatement through understanding the entity and its environment
	ISA 320 – Materiality in planning and performing an audit
Responding to risk stage	ISA 330 – The auditors responses to assessed risks
	ISA 500 – Audit Evidence
	ISA 530 – Audit Sampling
Concluding stage	ISA 450 – Evaluation of misstatements identified during the audit
	ISA 700 – Forming an opinion and reporting on financial statements
	ISA 705 – Modifications to the opinion in the independent auditor's report

The important thing to remember about the ISAs is that they set the standards to which the auditor must adhere. If an auditor is accused of being negligent in the performance of his duties, his best defence is to be able to prove that he complied with the standards in an appropriate manner.

PRELIMINARY ENGAGEMENT ACTIVITIES

1. Pre-conditions for an audit

1.1 In terms of ISA 210 – Agreeing the Terms of Audit Engagements, the objective of the auditor is to accept or continue an audit engagement only when the basis upon which it is to be performed has been agreed, through

* establishing whether the pre-conditions for an audit are present.
* confirming that there is a common understanding between the auditor and management and those charged with governance of the terms of the audit engagement.

Obviously if these two requirements cannot be established or confirmed, the auditor need go no further in considering accepting the engagement.

1.2 The pre-conditions for an audit are that

* the financial reporting framework to be applied in the preparation of the financial statements to be audited is acceptable. In South Africa the framework (suitable criteria) will normally be IFRS or IFRS for SMEs.
* the auditor obtains the agreement of management, that management ***acknowledges*** and ***understands*** its responsibility
  - For the preparation and fair presentation of the financial statements in accordance with IFRS or IFRS for SMEs whichever is appropriate for the company.
  - For such internal control as management determines is necessary to enable the preparation of financial statements that are free from material misstatement whether due to fraud or error.
  - To provide the auditor with access to all information of which management is aware that is relevant to the preparation of the financial statements such as records, documentation and other matters, ***including*** additional information that the auditor may request from management for the purposes of the audit, ***and*** unrestricted access to individuals within the company from whom the auditor determines it necessary to obtain audit evidence.

2. Prospective clients and continuance with an existing client

Once it is satisfied that the pre-conditions for the audit have been met, the audit firm should determine whether it wishes to establish or continue a relationship with the prospective client. Remember that an audit firm is itself a business, and therefore will not want to enter into a relationship if negative consequences are likely to flow. There are reasons that an audit firm may ***not*** wish to enter into a relationship with a prospective client :

* the client's management may appear to be unethical or lacking in integrity
* the audit firm may not wish to be associated with the "industry" or line of business in which the client operates, e.g. tobacco, pornographic materials, businesses which pollute the environment
* the client may have a reputation for poor relationships with its auditors and there may be a high risk of the auditor being sued for negligent performance
* it may be a sound business decision ***not*** to take on the client, e.g. the client doesn't pay the audit fee!
* the firm may not have the competence and resources to service the client properly.

Both the decisions about the pre-conditions for an audit and about the desirability of the relationship will be far easier to answer where the decision is about continuing a relationship. However the auditor will still give consideration to the above questions before continuing the engagement.

3. Compliance with Standards.

Whether it be for a prospective or existing client, ISA 220 – Quality control for an audit of financial statements, requires that the engagement partner be satisfied that appropriate procedures regarding the acceptance and continuance of client relationships and audit engagements have been followed, and that conclusions drawn in this regard, are appropriate. The engagement partner (firm) must:

3.1 Consider the ***integrity*** of the client's principal owners, key management and those charged with governance of the entity. This would include evaluating

* the business reputation of individuals described above, e.g. principal owners
* the client's business practices, including whether it could be involved in any criminal activities such as money laundering
* the attitude of the individuals described above, e.g. principal owners, to applying the "fairest" accounting standards as opposed to aggressively applying those which present the "most favourable picture"
* the client's attitude to paying audit fees, e.g. its willingness to pay fair fees, its aggressiveness in keeping fees low
* the possibility that the client will attempt to impose limitations on the audit, e.g. restrict access to certain information or individuals
* the identity and business reputation of related parties, e.g. subsidiary companies
* in the case of a prospective client, the reasons for the change of auditors
* management's attitude to sound corporate governance requirements, e.g. King III.

3.2 Determine whether the firm is ***competent*** to perform the engagement. This will require an assessment of whether the audit firm has

* personnel who have knowledge of the client's industry and the necessary experience of relevant regulatory and reporting requirements
* the necessary technical skills and competence within the firm, or the necessary access to other auditors or experts who do have the skills
* the necessary resources. For example, taking on a new client may mean that the audit firm has to employ more staff, particularly at busy periods such as year-end. Computer resources may also be an important consideration. Does the audit firm have sufficient hardware and software, as well as the technical computer skills, to offer the service?
* the personnel necessary to perform quality control reviews.
* the combined resources to meet the engagement reporting deadline.

3.3 Determine whether the firm can comply with ***ethical*** requirements. This will require that the firm evaluate whether

* there are any (potential) conflicts of interest between the firm and the client. A prospective client and the audit firm offer the same services to the same market, e.g. IT consulting, software distribution
* there are any threats to the independence of the firm, the engagement partner and the audit team (including external experts) and if adequate safeguards can be put in place to address any threats
* any other situations which might lead to contraventions of the Code of Professional Conduct by any member of the audit team, e.g. possible confidentiality threats where a prospective client is in direct competition with an existing client.

4. Procedures to gather "preliminary engagement" information.

Obviously in the case of an existing client, gathering information about the pre-conditions for an audit and whether to continue the relationship is far easier as the information is far more readily available. Generally speaking, this process is underway from the moment the initial engagement with the client commenced. As time passes, the firm gains a better understanding of the integrity of client, management's attitude to financial reporting and corporate governance, and whether the audit firm itself has been able to satisfy the competence and resource requirements. Equally, it is obvious that where the evaluation is being conducted on a prospective client, it is far more difficult to obtain the necessary information. However, the following procedures should provide sufficient information to make the decision:

4.1 Communication with the previous auditor (in compliance with the Code of Professional Conduct)

4.2 Discussion with the client's directors, senior financial personnel, audit committee, etc.

4.3 Inquiry of the firm's bankers, legal counsel etc. (permission would have to be sought)

4.4 Background searches of relevant databases, e.g. on the Internet

4.5 Review of any documentation, either public or made available by the prospective client, e.g. group reports, management reports

4.6 With regard to independence, enquiry and analysis of the status of the firm and its employees in relation to the potential client. (Firms should regularly request written information from their staff as to, for example, any family or personal relationships with, or investments in the firm's clients).

Note: where the client has an audit committee (e.g. a listed company), the audit committee will also be looking at the suitability of the audit firm, so there is likely to be a lot of co-operation between the committee and the firm.

5. Establishing an understanding of the terms of the engagement.

This is the formalizing of the terms of the engagement into the engagement letter which, in turn is a reflection of the presence of the pre-conditions for the audit. It is not a matter of simply drafting the letter and having it signed. Important aspects of the engagement are spelled out in the letter and it is important that the client (often represented by the audit committee), understands the terms. Whenever an auditor enters into an agreement to render services to a client, there is the possibility that the client (or the auditor) will misunderstand the nature of the engagement and the responsibilities of the parties involved. A client may not be entirely sure of what type of engagement is being undertaken. For example, the client may believe that an audit engagement which will result in an opinion given in a positive form, is being carried out, when in fact a review is being undertaken where a conclusion, expressed in a negative form, and not an opinion will be given. Clients may believe that the objective of an audit is to detect fraud, whilst others may be confused by terminology, e.g. independent review, compilation engagement, agreed upon procedure engagements and so on! This issue has in prior years been referred to as the "Expectation Gap"; very simplistically this means that clients often do not understand what the audit, or other services being rendered, are about and therefore expect certain assurances which they will not receive.

With the introduction of the "public interest score" concept there is likely to be more confusion on the part of some private company and close corporation clients who don't understand why they should have to be audited or, in the case of a private company, whether they are being audited or independently reviewed.

ISA 210 – Agreeing the terms of audit engagements, establishes and provides guidance on the "engagement letter standard" stating that "***the auditor shall agree the terms of the audit engagement with management or those charged with governance***". Note that this does not mean that the client negotiates with the auditor on what to do or how to do it. It is the right and duty of the auditor to decide on how the audit will be conducted.

The engagement letter is not a case of "one document fits all"; audits differ in extent and complexity, and have different terms and conditions. ISA 210 para 10, A23 and A24 provide guidance on what should be included in an engagement letter as well as additional matters which could be included depending on the circumstances of the audit. The following matters (points 5.1 to 5.5) as a minimum should be included in the engagement letter:

5.1 The ***objective*** of the audit should be clearly stated i.e. to express an opinion on the financial statements.

5.2 The ***scope*** of the audit should be conveyed by identifying the financial statements on which the opinion will be expressed and what they comprise, e.g. statement of financial position, statement of cash flows, etc. Reference may also be made to any legislation or regulations which may influence the scope of the audit, e.g. the Companies Act 2008 or the JSE requirements for the audit of listed companies.

5.3 The ***responsibilities of the auditor*** including:

* a statement that the audit will be carried out in terms of the ISAs and that the ISAs require that the auditor comply with ethical requirements
* a statement that the audit is planned and performed to provide ***reasonable assurance*** about whether the financial statements are free from material misstatement

* a broad description of the procedures conducted on an audit including a clear statement that the procedures selected depend on the auditor's judgement (emphasizing audit independence)
* an explanation that because of the ***inherent limitations of an audit*** together with the ***limitations of internal control***, there is an unavoidable risk that some material misstatements may remain undetected, even though the audit is properly planned and performed in accordance with the ISAs
* a clear statement that whilst the auditor considers internal control in order to design audit procedures, ***no*** opinion on the effectiveness of internal control is expressed ***but*** that weaknesses (significant deficiencies) identified in internal control relevant to the audit will be communicated to management.

5.4 The ***responsibilities of management*** including a statement that the audit will be conducted on the basis that management and those charged with governance ***acknowledge and understand*** that they are responsible for:
* the preparation and fair presentation of the financial statements in terms of IFRS or IFRS for SMEs
* such internal control as they deem necessary to enable the preparation of financial statements which are free from material misstatement
* providing the auditor with access to records, documents and other matters including additional information the auditor might request as well as unrestricted access to individuals within the entity from whom the auditors deem it necessary to obtain audit evidence.

5.5 Reference to the expected form and content of any reports to be issued by the auditor e.g. we expect that the report to be issued will state that in our opinion the financial statements, present fairly, in all material respects the financial position of the company at reporting date, and its financial performance and cash flows for the year then ended in accordance with IFRS and the Companies Act of South Africa. The report will be addressed to the shareholders and will contain an introductory paragraph, a paragraph dealing with the directors responsibility for the financial statements and a paragraph dealing with the auditor's responsibility.
However, this reference must include a statement that there may be circumstances in which the report will differ from its expected form and content.

The following matters may also be raised in the engagement letter (parts 5.6 to 5.10):

5.6 The auditor's expectation of ***written*** confirmation of oral representations.

5.7 Arrangements regarding the planning and performance of the audit, including
* the name of the ***designated auditor*** (Sec 44(1) of the Auditing Professional Act 2005) and the composition of the team for the audit engagement
* important dates for meetings with key personnel
* inventory counts
* audit deadlines.

5.8 Acknowledgement by management that they will inform the auditor of facts that may affect the financial statements, of which management may become aware during the course of the audit and during the period from the date of the auditor's report to the date the financial statements are issued.

5.9 When relevant arrangements concerning the involvement of other parties in the audit
* other auditors
* experts
* internal auditors
* predecessor auditor.

5.10 The basis of fee computation and any invoicing arrangements e.g. fees to be charged monthly.

The letter should conclude with a request to the client to sign and return an attached copy of the engagement letter as an acknowledgement of and agreement with the arrangements for the audit and the respective responsibilities of the auditor and management.

PLANNING

1. Introduction

ISA300 – Planning an audit of financial statements, states that the objective of the auditor is to: ***"plan the audit so that it will be performed in an effective manner"***. This entails developing an audit strategy, supported by an appropriate audit plan.

ISA 300 also requires that the engagement partner and other key members of the audit team be involved in planning the audit, as their experience and insight will enhance the effectiveness and efficiency of the planning process.

The importance of planning cannot be over-emphasised:

* proper planning helps to ensure that appropriate attention is devoted to important areas of the audit, e.g. significant risks are identified and addressed
* potential problems are identified and resolved on a timely basis, e.g. the client is implementing new financial reporting systems which may disrupt the current audit
* a competent and capable audit team, including other parties, e.g. experts, other auditors, who may be required on the audit, is assembled
* work can be properly assigned to audit team members, so that
  - the audit is effectively and efficiently performed
  - audit deadlines are met
* proper procedures for direction, supervision and review can be set up to meet quality control standards, including to the extent they are applicable to component (other) auditors and experts.

As explained earlier when we discussed the audit process, planning should not be seen as a "stand alone" stage of the audit; neither the overall audit strategy nor the audit plan, is static. As circumstances change on the audit, so may the overall strategy and audit plan change. For example, unexpected problems encountered on the audit of work-in-progress may necessitate engaging an expert, something that was not considered when the overall audit strategy was formulated. This in turn may lead to more intensive audit procedures of a different nature being carried out. In addition, as the current audit unfolds, planning for the following year's audit should be underway as a natural "by-product" of the audit being conducted.

2. The overall audit strategy

2.1 The overall audit strategy sets the ***scope, timing and direction*** of the audit and guides the development of the ***audit plan.*** To establish the overall audit strategy, the key engagement team members must

* determine the characteristics of the client company which will define the scope of the engagement, e.g. where the client is a listed company, JSE listing requirements and the King III Report requirements will affect the scope of the engagement (see also 2.3 below)
* determine the reporting objectives of the engagement which will influence the ***timing*** of the audit, e.g. reporting deadlines, scheduled meetings with the audit committee (see also 2.4 below)
* consider the important factors that will determine the focus or ***direction*** of the audit, e.g. results of previous audits, account headings which attach higher risk of misstatement (see also 2.5 below)
* consider any aspects of the preliminary engagement activities which may affect the audit strategy e.g. concerns over the competence/experience of senior accounting personnel (see also 2.5 below)
* ascertain the resources necessary to perform the engagement
  - the resources to be allocated to specific audit areas – e.g. level of staff experience required, use of experts

- the amount of resources to be allocated, e.g. the number of staff to be allocated to the inventory count
- the timing of the allocation of resources, e.g. at an interim stage, and
- how the resources are to be managed, directed and supervised, e.g. meetings, evaluations, quality control reviews.

2.2 In formulating the audit strategy, key engagement team members should consider matters such as those listed in 2.3 to 2.5 below (this list is not exhaustive and is for illustrative purposes; reference should be made to ISA 300).

2.3 Characteristics of the engagement which define its scope

* the financial reporting standards on which the financial information to be audited, has been prepared
* the expected audit coverage, including the number and locations of components to be included, e.g. divisions, inventory storage locations
* the involvement of other auditors, e.g. holding company auditors and their requirements
* the need for specialized knowledge of the client's industry or reporting
* the availability of the work of internal auditors and the extent of the auditor's potential reliance on such work
* the effect of information technology on the audit procedures, including the availability of data and the expected use of computer-assisted audit techniques
* whether the engagement includes the audit of consolidated financial statements.

2.4 Matters which will affect the reporting objectives, timing of the audit and nature of communications

* the company's timetable for reporting, e.g. interim and year-end financial reporting deadlines
* the schedule of meetings with management and those charged with governance including the audit committee, where applicable, to discuss the nature, extent and timing of the audit work
* the expected type and timing of reports to be issued, including the auditor's report, management letters and communications to those charged with governance
* communication with component (other) auditors, experts, internal audit, regarding the expected types and timing of reports to be issued as a result of their work on the audit
* the size, complexity (e.g. complex manufacturing facilities) and number of locations of the client. This will affect the timing of visits to the client
* the extent and complexity of computerization at the client e.g. availability of data and personnel for assistance with CAATs may also affect the timing of visits to the client.

2.5 Matters that determine the focus of the engagement team's effort and direction of the audit

* materiality levels, stricter levels result in more audit work
* preliminary identification of areas where there may be a higher risk of material misstatement
* the presence of significant risks
* the impact of the assessed ***risk of material misstatement at the overall financial statement leve***l on direction, supervision and review, e.g. high risk at financial statement level may require more experienced staff to be assigned to the audit, and more intense supervision and reviews to be conducted
* evidence of management's commitment to the design and operation of sound internal control e.g. strong commitment may equal more reliance by the auditor on internal controls
* the volume of transactions, which may determine whether it is more efficient for the auditor to rely on internal control, and which may dictate the use of CAATs
* significant business developments affecting the entity which have recently occurred, including changes in information technology, in key management, in industry regulations and in applicable accounting standards.

The initial audit strategy will be set by considering the points above, but don't forget that this "preliminary" strategy will be influenced by the identification and assessment of the risk of material misstatement at assertion level as well. This is because the auditor will learn much more about the client when carrying out these identification and assessment procedures which in turn will enable him to refine the audit strategy.

3. The audit plan itself

3.1 The audit strategy and the audit plan (which we must think of as two plans, see 1.2 on page 6/7), are closely interlinked, but the audit plan is far more detailed than the overall strategy. Many of the factors which will influence the audit strategy, will also influence the audit plan. For example, Tonnes Ltd holds large quantities of inventory in a number of locations. Part of the ***overall audit strategy*** is to make use of other firms of auditors to, inter alia, attend the year-end inventory counts at the various warehouses. The audit plan will now need to address this decision by defining the nature, timing and extent of procedures that will have to be carried out by the other auditors, e.g. attend inventory counts, and on the work conducted by them e.g. how the audit team communicates with the other auditors and how their work is reviewed and problems resolved.

3.2 In terms of ISA 300, the audit plan must contain:

* a description of the nature, timing and extent of planned ***risk assessment procedures,*** sufficient to assess the risks of material misstatement (plan 1)
* a description of the nature, timing and extent of planned ***further audit procedures*** at the assertion level for each material class of transactions, account balance and disclosure (plan 2)
* any ***other audit procedures*** which may be required to comply with the ISAs (plan 2)

In addition, a plan must also be compiled regarding the nature, timing and extent of the ***direction and supervision of the audit team,*** and the ***review*** of their work.

3.3 It should be obvious to you that before the audit strategy, and particularly the audit plan, can be effectively developed, a great deal of information about the client company is required. We cannot plan the audit if we have not obtained an understanding of the entity and its environment.

Simplistically, modern auditing is about identifying the risks of material misstatement and responding to those risks in such a manner that audit risk is reduced to an acceptable level. To extend our example above : having performed the risk assessment, the audit team believes that Tonnes Ltd may attempt to overstate their inventory on hand so as to manipulate reported profits. The audit plan must respond to this by detailing procedures which will identify instances where fictitious (non-existent) inventory, or inventory not owned by Tonnes Ltd, has been included in the year-end inventory figures. The other auditors attending the inventory counts on our behalf, must be made aware of the risk (of overstatement) and instructed on the nature, timing and extent of the tests which must be carried out. These may include extending the number of items counted, and performing extensive year-end cut-off tests, at the warehouses. Of course we may assess that the directors' desire to manipulate profits is a risk at overall financial statement level and that other account headings are also directly at risk. An appropriately competent and experienced audit team must be put in place and the audit plan must include further audit procedures to respond to the risk at assertion level.

4. Materiality

As indicated above, the audit is geared towards identifying the risk of ***material*** misstatement. It follows therefore, that before the audit strategy and particularly the audit plan can be developed, the auditor will need to give some attention to determining "what is material" for the audit. For example, the audit team cannot effectively plan procedures to identify and assess risk of material misstatement if they do not have an idea about what is material. This is discussed in detail in Chapter 7.

5. Planning and conducting risk assessment procedures

A point that has been made a number of times is that the auditor must have a thorough understanding of the client company and the environment in which it operates. This is especially important for the purposes of identifying and assessing risk. If the auditor does not understand the client and its

business, he will be unable to adequately identify and assess the risk of material misstatement. Understanding the entity and its environment is covered in detail in chapter 7. The auditor must assess:

5.1 Risk at financial statement level

ISA 315 (Revised) requires that the risk of material misstatement be identified and assessed at financial statement level and at assertion level. Risk at the financial statement level is the risk which affects the financial statements as a whole, and which filters down into the account balances and totals which make up the financial statements. It is the risk that pervades the financial statements. For example, if the client's management lacks integrity, the audit as a whole is inherently more risky than for the audit of a client whose management has a proven record of integrity. The effect of managements' lack of integrity may filter down into the financial statements as they attempt to manipulate the account balances and totals to suit their own purposes. Risks of this nature often relate to the client's control environment and are not necessarily identifiable with specific assertions at transaction, account balance or disclosure level. However, the auditor needs to consider carefully how high risk at financial statement level may affect risk at assertion level.

Although chapter 7 deals with the information the auditor will seek to gain an understanding of the client, the following list illustrates the kind of information which might have an affect on the identification and assessment of risk at the financial statement level.

* the integrity of management
* Management's experience and knowledge, for example, the financial reporting inexperience of management may affect the preparation of the financial statements of the entity
* unusual pressures on management, for example, circumstances that might predispose management to misstate the financial statements, such as the company facing going concern problems or management bonuses being linked to financial performance
* the nature of the entity's business, for example, the significance of related parties, and the influence its shareholders (such as a holding company) may have on its financial reporting.

5.2 Risk at assertion level

This relates to the risk of misstatement at the assertion level for classes of transactions, account balances and disclosures. It is therefore essential that the auditor gather information which will enable him to identify and assess risk for each of the assertions applicable to the transactions, account balances and disclosures which are included in the financial statements. Again, chapter 7 deals with the information the auditor will seek to be in a position to identify and assess risk of material misstatement at the assertion level, but the following examples have been included to illustrate the point.

* information about the products the company sells, whether it sells to related parties, how sales are initiated, recorded and processed. What documentation there is relating to the sale which will assist the auditor in identifying and assessing the risk of material misstatement arising from the inclusion of sales which have not actually occurred or which do not pertain to the entity i.e. the ***occurrence assertion relating to a class of transaction***.
* information about the type of inventory held, the locations at which it is held, the physical and other controls and the nature, extent and reliability of the records detailing the movement of inventory will assist the auditor in identifying and assessing the risk of material misstatement arising from the inclusion of inventory which does not exist in the inventory account balance i.e. the ***existence assertion relating to an asset account balance***.
* information about related parties, director's interests in contracts, pending litigation, share options and incentive schemes for directors (inter alia), will assist the auditor in identifying and assessing the risk of material misstatement arising from the omission of disclosures which should have been included in the financial statements i.e. the ***completeness assertion relating to presentation and disclosure.***

Of course information gathered will frequently relate to more than one assertion and part of the skill of a good auditor will be the ability to link the information to the risk of material misstatement for all assertions that may be affected. Also remember that information pertaining to the assessment of material risk at the financial statement level may influence the assessment at assertion level. For example, if information gathered suggests that management may be predisposed to manipulate the financial statements, the risk of material misstatement relating to the ***occurrence of sales*** will increase because management could manipulate the financial statements by including fictitious sales.

6. Planning "further" audit procedures based on the risk assessment

As indicated earlier, the auditor's first response to assessed risk is to plan further audit procedures. This will entail developing a plan which describes the nature, timing and extent of further audit procedures, both tests of controls and substantive tests, which will be conducted to reduce the risk of material misstatement relating to the assertions remaining undetected.

6.1. Some general observations relating to the nature, timing and extent of further audit procedures

* the nature of an audit procedure relates to its purpose, i.e. test of controls or substantive, and its type, i.e. inspection, observation, inquiry, recalculation, reperformance, analytical procedure or external confirmation.

* tests of controls can only be carried out where the system is "worthy" of being tested, e.g. if the system by virtue of weaknesses in its design or implementation, is not effective, there is little point in testing it. There must be an expectation that controls are operating effectively before testing them.

* a single test of controls is virtually never sufficient. For example, ***observing*** a receiving clerk count goods received and comparing the quantity to the supplier delivery note, only tells you that the control was carried out on the occasions that you observed him. Once you leave the receiving bay, he may not carry out the control procedure. ***Inquiry*** conducted in isolation will also provide insufficient evidence. Further evidence which supports the response to the inquiry, is required.

* if the auditor is trying to gain evidence about the effective functioning of controls over a period of time (this is normally the case), tests of controls will have to be conducted at various times during the period. It cannot be assumed that because controls were working effectively in April, they will be working effectively in August. There are of course factors which may reduce the risk that controls are not working effectively over time, e.g.
  - where there is a strong ongoing control environment
  - extensive monitoring of controls has taken place during the period
  - strong general controls, particularly in computerized systems
  - minimal changes in the business have occurred.

* irrespective of the assessed risk of material misstatement, the auditor must design and perform substantive tests for each ***material*** class of transactions, account balance and disclosure. Tests of controls cannot in themselves, provide sufficient, appropriate evidence.

* where ***significant*** risks (these are risks which require special audit consideration) are identified, the auditor must perform substantive tests which specifically address the risk. These tests must include tests of detail and cannot be purely analytical procedures.

* the auditor's substantive procedures must include the following in respect of the financial statement closing process
  - agreeing or reconciling the financial statements with the underlying accounting records, and

- examining material journal entries and other adjustments made during the course of preparing the financial statements.

* the timing of tests is frequently dictated by key dates at the client and the objective of the test. For example
  - a tight audit deadline may result in a comprehensive interim audit, supplemented by "roll forward" tests.
  - the attendance at an inventory count is obviously determined by the date the client conducts the year-end inventory count
  - subsequent events can only be audited in the post-balance sheet period
  - the availability of client IT staff may affect the timing of using computer assisted audit techniques.

* in general terms, a greater risk of material misstatement will result in more testing
  - where internal controls prove to be ineffective, the extent (and possibly the nature) of substantive testing will increase
  - the extent of testing is usually expressed in terms of sample size. Sample size can be determined by professional judgement or more sophisticated statistical sampling plans
  - the use of CAATs will usually enable the auditor to test far more extensively as a result of the power, versatility and speed of computers and audit software.

* an effective audit plan will be a combination of tests of controls and substantive tests, as well as a mix of the different types of test, e.g. inspection, analytical review, etc.

* ***the chart which follows*** is an attempt to illustrate what the auditor might consider when deciding on the nature, timing and extent of "further" audit procedures. Don't forget that many of the points raised in paras 2.1 to 2.5 under the overall audit strategy on pages 6/13 and 6/14 will also have a bearing on the nature, timing and extent of further audit procedures.

Developing an audit plan is not always straightforward, and the larger and more complex the client, the harder it is. Professional judgement and experience will play a large part in blending tests of controls, substantive testing and other ISA procedures into a plan which meets the standard i.e. "a plan which will ensure the audit is performed in an effective manner so as to reduce audit risk to an acceptable level."

CHARACTERISTIC	*MATTERS TO CONSIDER*
nature of tests – what tests will be conducted?	* the suitability of a particular procedure to provide the piece of evidence required • reperformance, inspection, inquiry, observation • recalculation, analytical procedures, external confirmation * the need to perform tests of detail (e.g. significant risks) * the possibility of performing analytical procedures exclusively (for certain aspects of the audit) * the hierarchy of evidence – how can the most relevant and reliable evidence be gathered? * statistically based or non-statically based sampling * the use of other parties • experts, other (component) auditors, internal auditors * the use of computer assisted audit techniques • system or data orientated CAATs * special client requests e.g. the client has asked you to perform special cash counts * do the tests selected, address the risk adequately?
timing of tests – when will the tests be conducted?	* the need for and desirability of • interim audits • early verification of year end balances combined with "roll forward tests", e.g. debtors circularisation carried out two months prior to year end, supplemented by tests of controls, tests of detail and analytical procedures for the subsequent period of two months up to reporting date * preparatory work on 3rd party confirmations and supporting schedules * non-negotiable dates set by client • inventory count • reporting deadlines • availability of key personnel • audit committee meetings * availability of information, e.g. fixed asset schedules for audit, including final information for analytical procedures * timeous preparation where other parties will be used, e.g. an auditor cannot contact an expert the week before the year-end inventory count to assist in the valuation of say, work-in-progress * special client requests e.g. the client may request that you visit each branch to attend inventory cycle counts at least once a year.
extent of tests – how much testing is to be done?	* level of assessed risk * prior year experience * the planning and performance materiality limits which have been set – as the level of misstatement which the auditor believes would influence a user reduces, so the extent of testing increases * what sample sizes are required to achieve meaningful results (particularly when non statistically based sampling is used) * possible reduction of testing when internal audit is used * 3rd parties to understand "how much" they should do * special client requests e.g. positively confirm ***all*** debtors * the extent of testing deemed necessary should not be restricted by deadlines

RESPONDING TO ASSESSED RISK

Having responded initially to the risk assessment by planning further audit procedures, the auditor will proceed by implementing an overall response and by carrying out the planned "further" and "other" procedures.

1. Overall response at financial statement level

In terms of ISA 330 – The auditor's responses to assessed risks, the auditor shall design and implement ***overall responses*** to assessed risks of material misstatement at ***financial statement level***, and should design and perform ***further*** audit procedures to respond to assessed risks ***relating to the assertions*** (at account balance/transaction and disclosure level)

1.1 ***Overall responses*** – these are not really procedures but rather general actions to deal with risk at financial statement level. For example, if the auditor is concerned with management's integrity, the overall response may be to meet with the audit team to emphasise the need to maintain a high level of professional scepticism, and to assign experienced and strong willed staff to the audit. Obviously it does not end there. The potential effect of management's lack of integrity on the assertions at account balance/class of transaction/disclosure level will need to be evaluated, and the appropriate procedures implemented (nature, timing and extent). For example, the auditor's concern may be that management will manipulate the financial statements by overstating the value of inventory on hand at year-end and by including fictitious sales. The auditor would respond by conducting extensive procedures on the existence, rights and valuation of inventory and the occurrence of sales/existence of debtors.

1.2 Overall responses may be summarized as follows

* emphasize professional scepticism
* assign more experienced staff with special skills or use experts
* provide more supervision
* incorporate elements of unpredictability into the audit procedures adopted (do things in a manner which the client may not expect), e.g. surprise visits to client
* make general changes to the nature, timing and extent of audit procedures conducted in the past.

2. Audit procedures to respond to the assessed risks of material misstatement at the assertion level (further procedures)

2.1 Generally these procedures will form the major part of any audit although some practitioners might argue that planning takes up the major portion! They are the procedures to be carried out to respond to the risk of material misstatement pertaining to the assertions. Remember that the assertions are the representations applicable to the various account headings, classes of transaction and disclosures which underlie the financial statements, e.g. the ***valuation*** of inventory, plant and equipment, the ***existence*** of debtors, the ***completeness*** of sales, the ***understandability*** of a contingent liability disclosure, etc. The auditor must respond to the risks by getting the nature, timing and extent of tests of controls and substantive tests correct so as to reduce the risk of material misstatement going undetected to an acceptable level, and ultimately reducing the risk of expressing an inappropriate opinion. In other words, the auditor carries out further audit procedures with the intention of reducing audit risk to an acceptable level.

2.2 This is the stage at which the auditor makes use of the major tools in his toolbox – tests of controls and substantive tests, and it is perhaps useful to recall what these tests entail.

* ***Inspection :*** consists of examining records, documents (physical files or electronic storage media), or tangible assets, e.g. inspecting the minutes of directors' meetings for evidence of the approval of a major investment transaction, inspecting the client's machinery for damage (impairment) or existence

* ***Observation :*** consists of looking at a process or procedure being performed by others, e.g. the observation by the auditor of the counting of inventories by the entity's personnel or observing the receiving clerk counting and checking goods being delivered to the company by a supplier

* ***Inquiry :*** consists of seeking information from knowledgeable persons inside or outside the entity

- inquiries may range from formal written enquiries addressed to third parties, to informal oral enquiries addressed to persons inside the entity, e.g. a receiving clerk may be asked what controls are exercised when goods are received from a supplier

* ***External confirmation :*** amounts to the obtaining of a direct written response to an enquiry to corroborate (confirm) information contained in the accounting records, e.g. the auditor may seek direct confirmation of amounts owed, by communication with debtors

* ***Recalculation :*** consists of checking the mathematical accuracy of documents or records or of performing independent calculations, e.g. checking that discounts have been correctly calculated on sales invoices, or recalculating interest accrued

* ***Analytical procedures :*** consist of the analysis of significant ratios and trends, ***including*** the resulting investigation of fluctuations and relationships that are inconsistent with other relevant information or which deviate from predicted amounts, e.g. comparing the current ratio for the year under audit, to the prior year current ratio, and seeking an explanation if there is a difference

* ***Reperformance :*** is the auditor's independent execution of procedures or controls that were originally performed as part of the entity's internal control, e.g. reperforming the year-end bank reconciliation.

In addition to ISA 500 – Audit Evidence, which describes the types of procedures available to gather evidence, there are numerous statements which give guidance on the audit of specific matters. For example, how to audit accounting estimates (ISA 540), and how to conduct analytical procedures (ISA 520). Remember the objective is to gather sufficient (enough) appropriate (relevant and reliable) evidence to reduce the risk of material misstatement remaining undetected in the account balances, classes of transactions and disclosures which make up the financial statements, to an acceptable level. Combinations of procedures are carried out and are often referred to by a collective name, e.g. carrying out a debtors circularization to assist in verifying the existence of debtors, or conducting cut-off procedures on sales at year-end, to test the assertions of occurrence and completeness.

3. Audit procedures carried out to satisfy the requirements of the ISAs (other procedures)

3.1 You will recall that in terms of ISA 300, the audit plan must include (the nature, timing and extent of) procedures which the auditor is required to carry out arising from the important need to comply with the standards. These procedures do not arise directly from the risk assessment but may be linked to it. For example, ***risk assessment procedures*** may reflect that there is no risk surrounding the going concern ability of the company. This does not mean that the auditor can ignore ISA 570 - Going concern, and simply accept that there is no going concern problem based on the risk assessment. The statement requires that the auditor gather sufficient, appropriate evidence to support management's decision to use the going concern assumption in the preparation of the financial statements. Other standards which must be complied with are, for example, ISA 260 and ISA 265 which deal with communicating with those charged with governance and communicating deficiencies in internal control to the client.

EVALUATING, CONCLUDING AND REPORTING

Something has to be done with the audit evidence gathered. ISA 700 – Forming an opinion and reporting on financial statements, states that the auditor should form an opinion on the financial statements based on an evaluation of the conclusions drawn form the audit evidence obtained. This is carried out in this stage of the audit process. The evaluation sets out to determine whether:

1. Sufficient, appropriate evidence has been obtained to reduce audit risk to an acceptable level.

* ISA330 – The auditor's responses to assessed risks, requires that the auditor conclude on whether sufficient, appropriate audit evidence has been obtained to reduce audit risk to an acceptably low level. The auditor is required to consider all evidence, not just that which corroborates the assertions. If evidence contradicts say, the existence assertion relating to debtors (i.e. the evidence suggests there may be fictitious debtors included in the balance) the auditor must consider this evidence and respond by seeking further evidence. If the auditor is unable to obtain sufficient appropriate audit evidence, a qualified opinion or a disclaimer of opinion will have to be issued. Bear in mind that audit risk is the risk that the auditor expresses an inappropriate audit opinion when the financial statements are materially misstated, e.g. the auditor's opinion is that the financial statements "present" fairly when in fact they are materially misstated.

2. Uncorrected misstatements which have been identified during the audit, result either individually or in aggregate, in a material misstatement of the financial information.

* In terms of ISA 450 – Evaluation of misstatements identified during the audit, a ***misstatement*** is a difference between the amount, classification, presentation or disclosure of a reported financial statement item and the amount, classification, presentation or disclosure that is required for that item in terms of the applicable accounting framework e.g. IFRS. Simplistically expressed, a misstatement is a difference in what ***has*** been reported (by the directors) in the financial statements, and what ***should*** have been reported in terms of the reporting framework e.g. a particular lease has been reported as a finance lease when in fact it does not meet the criteria for classification as a finance lease, or inventory has been valued and reported at replacement cost and not at the lower of cost or net releasable value, or a material contingent liability has not been disclosed. Misstatements may arise out of fraud or error.

* In terms of ISA 450, the auditor must document all misstatements in the work papers (audit documentation) and must indicate whether they have been corrected. The auditor must also conclude on whether uncorrected misstatements are material, individually or in aggregate. Misstatements that are clearly trivial may be ignored.

* This work paper is often referred to as an "overs and unders" schedule. The figures on the schedule should be supported by sufficient evidence for the manager or engagement partner to evaluate. Where necessary, discussions with members or the audit team will be conducted.

* An important distinction has to be made between misstatements which have been specifically identified and about which there is no doubt ***(factual misstatements)*** e.g. the total cost of certain inventory items has been incorrectly calculated, and those which, in the auditor's judgment, are likely to exist (***judgemental misstatements***), e.g. where estimation is involved such as allowances for inventory obsolescence. Judgemental misstatements are differences which arise between management's accounting estimates and what the auditor considers a reasonable estimate to be, e.g. management may consider that an inventory obsolescence allowance of R500 000 is appropriate but the auditor thinks that a reasonable allowance would be R750 000. The judgmental misstatement would be R250 000. Similarly a judgemental misstatement will arise where the auditor thinks that the selection or application of a particular accounting policy by management is inappropriate. This only applies where the accounting policy and its application are open to interpretation.

  The differences between the amounts (and disclosures) which the auditor thinks would be reflected in the financial statements if the appropriate policy was selected and applied, and the amounts and disclosures which have been reflected will be the judgemental difference(s). If the selection or application is just plainly wrong, it will be factual misstatement.

  The third type of misstatement is termed ***projected misstatement***. A projected misstatement is the auditor's best estimate of the amount of misstatement in a population based on the projection of the misstatement found in a sample taken from that population.

  It is important to distinguish between the different types of misstatement because the type of misstatement will affect how the auditor will react

* where there is a factual misstatement, the auditor is on solid ground when requesting the client to make adjustments to the financial statements and, if the adjustments are not made, when modifying the audit report (qualifying the audit opinion)
* where there is a judgemental misstatement, the auditor is on far less solid ground. The misstatement has only arisen because there is an element of interpretation in the facts. The auditor cannot state categorically that the directors are wrong! As a result the auditor may have to accept a measure of compromise when requesting adjustment and will have to think very carefully about whether and how to modify the report
* where there is a projected misstatement, the auditor may be in for an even harder time when requesting amendments or qualifying the audit report. Projecting misstatement over a population based on a sample can be a very subjective matter. If a proper statistical sampling method has been properly applied it is less subjective, but there is still plenty of subjectivity in setting the parameters for the sampling plan. A client is not going to be too happy with an auditor who says "we think, based on a projection of our sample, that the inventory balance is overstated by R500 000". The client is going to want more hard evidence than that! So again the auditor will need to accept a measure of compromise and think carefully about modifying the audit report.

* The materiality of the audit difference is a very important part of this evaluation. If an audit difference is regarded as not material (leaving the misstatement uncorrected will not influence a user's decision), the auditor will not insist on adjustment being made but will still bring it to the attention of the client who, of course, may choose to correct it.

3. ***The financial statements have been prepared in all material respects in accordance with the applicable financial reporting standards.*** In particular the auditor will evaluate whether:

* the financial statements ***adequately disclose the significant accounting policies*** selected and applied

* the accounting policies selected and applied are ***consistent*** with the financial reporting standards/accounting framework and ***appropriate*** for the company's business

* the ***accounting estimates*** made by management are reasonable

* the information presented in the financial statements is ***relevant***, ***reliable***, ***comparable*** and ***understandable***

* the financial statements provide adequate ***disclosures*** to enable users to understand the effect of material transactions and events on the entity's financial position, financial performance and cash flows (information conveyed in the financial statements)

* the ***terminology*** used in the financial statements is appropriate

* the company has complied with the applicable ***statutory requirements and regulations***, e.g. JSE regulations for listed companies and King III corporate governance requirements

* the financial statements achieve ***fair presentation.***

4. ***All material events occurring after the reporting date*** and up to the date of the audit report which may indicate the need for adjustment to, or disclosure in, the financial information on which the auditor is reporting, have been identified, and appropriately dealt with.

The evaluation as described above, will be carried out by a senior member of the audit team, probably the manager or engagement partner. During the course of the audit, evaluation and review will have taken place at various levels so that, in effect, this final evaluation will be of evidence (contained in the working papers) that has already been subject to scrutiny. Based on the evaluation, the manager/partner will conclude on whether an unmodified audit opinion is appropriate. If not, further decisions must be made as to whether an "except for" qualification, an adverse opinion or a disclaimer of opinion should be given. This is dealt with in the chapter on reporting (see Chapter 18). The engagement partner will also consider whether any other modifications such as the inclusion of an emphasis of matter paragraph, or a paragraph which reports on other legal and regulatory duties of the auditor, e.g. Sec 45 of the Auditing Profession Act 2005 (reportable irregularities), are required.

CHAPTER 7

IMPORTANT ELEMENTS OF THE AUDIT PROCESS

CONTENTS

UNDERSTANDING AUDIT RISK		7/4
INTRODUCTION		7/4
THE INHERENT LIMITATIONS OF AN AUDIT		7/4
THE LINK BETWEEN AUDIT RISK AND THE AUDIT PROCESS		7/4
THE COMPONENTS OF AUDIT RISK		7/5
1.	Inherent Risk	7/5
2.	Control Risk	7/5
3.	Detection Risk	7/6
4.	Relationships between the different risks and material misstatements	7/6
UNDERSTANDING THE ENTITY AND ITS ENVIRONMENT		7/7
INTRODUCTION		7/7
RISK ASSESSMENT PROCEDURES AND RELATED ACTIVITIES		7/8
1.	Client acceptance of continuance procedures	7/8
2.	Previous experience with the entity	7/8
3.	Inquiries of management	7/8
4.	Observation	7/9
5.	Inspection	7/9
6.	Analytical procedures	7/9
7.	Discussion among the audit team	7/10
8.	The required understanding of the entity	7/10
THE ENTITY AND ITS ENVIRONMENT		7/11
1.	Industry, regulatory and other external factors	7/11
2.	The nature of the entity	7/11
3.	The entity's selection of accounting policies	7/13
4.	The entity's objectives and strategies and related business risks	7/13
5.	Measurement and review of the entity's financial performance	7/13

THE ENTITY'S INTERNAL CONTROL 7/14

1. Control environment 7/14

2. The entity's risk assessment process 7/15

3. The information system 7/15

4. Control activities 7/19

5. Monitoring of controls 7/19

SIGNIFICANT RISKS 7/20

THE CONCEPT OF MATERIALITY 7/21

INTRODUCTION 7/21

THE NATURE OF MATERIALITY 7/22

1. Subjective 7/22

2. Relative 7/22

3. Quantitative and qualitative 7/23

PLANNING MATERIALITY AND PERFORMANCE MATERIALITY 7/24

1. Planning materiality 7/24

2. Performance materiality 7/25

3. Planning for qualitative misstatements 7/26

4. Revision of planning and performance materiality levels 7/27

MATERIALITY AT THE EVALUATING STAGE (FINAL MATERIALITY) 7/27

1. Introduction 7/27

2. Misstatements 7/27

3. Consideration of identified misstatements as the audit progresses 7/28

4. Evaluating the affect of uncorrected misstatements on the financial statements 7/28

CONCLUSION 7/31

THE AUDITOR'S RESPONSIBILITIES RELATING TO FRAUD IN AN AUDIT OF FINANCIAL STATEMENTS 7/32

INTRODUCTION 7/32

AUDITOR'S OBJECTIVE 7/32

TERMINOLOGY – DEFINITIONS 7/32

RESPONSIBILITY OF MANAGEMENT AND THOSE CHARGED WITH GOVERNANCE 7/34

RESPONSIBILITIES OF THE AUDITOR 7/34

RESPONSES TO THE RISK OF MATERIAL MISSTATEMENT DUE TO FRAUD 7/35

1. At financial statement level 7/35

2. At assertion level 7/35

3. Management override 7/36

4. Evaluation of evidence 7/37

5. Management representations 7/37

FRAUD RISK FACTORS 7/38

1. Introduction 7/38

2. Fraudulent financial reporting 7/38

3. Fraud risk factors relating to misappropriation of assets 7/40

COMMUNICATION WITH MANAGEMENT, THOSE CHARGED WITH GOVERNANCE AND OTHERS 7/41

1. Introduction 7/41

2. Parties with whom the auditor might communicate concerning fraud 7/41

FRAUD AND RETENTION OF CLIENTS 7/42

CONSIDERATION OF LAWS AND REGULATIONS IN AN AUDIT OF FINANCIAL STATEMENTS – ISA 250 7/43

1. Introduction 7/43

2. Important considerations 7/43

3. Auditor's duties, responsibilities and procedures 7/43

4. Reporting of non-compliance 7/44

UNDERSTANDING AUDIT RISK

INTRODUCTION

Before going into the detail of certain elements of the audit process we need to remind ourselves about the role the auditor plays and what is expected of the auditor. The auditor's role is to provide reasonable assurance about the fair presentation of the company's financial statements. Users want to be satisfied that the audited financial statements on which they are relying, are free of material misstatement and their reliance is an implied acceptance that the auditor has performed his function properly. However, there is always the risk that the auditor will "get it wrong" and give an incorrect opinion. This is audit risk. To define it more precisely, we can look to ISA 200 – Overall objectives of the independent auditor and the conduct of an audit in accordance with the International Standards on Auditing, which defines audit risk as ***the risk that the auditor will express an inappropriate opinion when the financial statements are materially misstated.*** In simpler terms, it is the risk that the auditor will give an unqualified opinion when in fact a qualified, adverse, or disclaimer of opinion should have been given.

THE INHERENT LIMITATIONS OF AN AUDIT

A valid question might be "if the auditor does his job properly, won't he eliminate the risk of expressing an appropriate opinion, or in other words reduce audit risk to zero?" The answer is that audit risk can never be completely eliminated due to the inherent limitations of an audit. These can be summarized as follows:

* ***the nature of financial reporting itself.*** The auditor is forming an opinion on financial statements which include a great deal of information which is based on judgement, subjective decisions and assessments.
* ***the nature of audit procedures***
  - there is always the possibility that management or others may not provide the auditor with complete information relating to the financial statements. Accordingly, the auditor can perform procedures related to the completeness of information but can never be 100% certain that all information has been recorded or conveyed to him.
  - fraud, including collusion and falsification of documents, may be so sophisticated and expertly hidden that conventional audit procedures will be ineffective in detecting misstatement
  - an audit is not an official investigation into wrongdoing, and accordingly the auditor does not have the legal powers which may be necessary to pursue certain evidence
  - most audit procedures are conducted on samples so there is always the risk that material misstatement will go undetected
* ***time constraints***
  - if the auditor had an unlimited amount of time to conduct the audit, audit risk could probably be significantly reduced. However, the relevance and value of information diminishes (rapidly) over time so the audit must be completed within a reasonable period after the financial year end. Clearly, time available should not be used as an excuse for not doing the audit properly and can be addressed, to a large extent by proper planning, but it does remain a limiting factor.
* ***cost/benefit***
  the same logic will apply to cost. It is too costly (and would take too long) to address all information and pursue every matter exhaustively, just to obtain that little extra bit of evidence when it will produce no real benefit.

However, despite its limitations, the audit remains a very important function.

THE LINK BETWEEN AUDIT RISK AND THE AUDIT PROCESS

The audit process is a combination of stages which the auditor goes through to be in a position to report on whether the financial statements are fairly presented. The audit process as it is today, has been developed over time by the profession in such a manner that if the process is followed, ***audit risk*** will be kept to an acceptable level. The International Standards on Auditing (ISAs) direct the audit process so it follows that compliance with the standards will result in audit risk being kept to an acceptable level. A clearer understanding of audit risk will help to put the audit process into context.

COMPONENTS OF AUDIT RISK

To better understand audit risk we need to understand its components. There are three "components" of audit risk, and in addition to defining these we must consider the relationship between audit risk and its components and the components themselves. ISA 200 provides the necessary guidance.

1. Inherent risk

Inherent risk is the susceptibility of an assertion about a class of transaction, account balance or disclosure, to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls. For example, transactions which require complex calculations e.g. complex lease agreements are ***inherently*** more likely to be misstated than simple transactions e.g. a purchase of goods. Of course as auditors we would expect the client to put controls in place to ensure that the complex transaction is correctly recorded, but the transaction remains "inherently risky". Another way of looking at it may be to describe inherent risk, as the "built in" risk which an account balance, class or transaction or disclosure might have. For example, there is more inherent risk relating to the ***valuation*** assertion for an inventory of diamonds in a jewellery business, than to the valuation assertion of an inventory of cricket bats at a sporting goods wholesaler. A cricket bat is, and looks like, a cricket bat, but a diamond has inherent characteristics which make it difficult to identify (is it glass or ziconia?) and to value (what number of carats it is, is it flawed, what colour is it?). The important thing is that the auditor must identify the inherent risk ***and*** respond to it. In this example an expert may be called in to assist the auditor in the valuation of the diamonds. Expressed another way, the risk of material misstatement is greater for an inventory of diamonds than it is for an inventory of cricket bats because of the inherent characteristics of diamonds compared to cricket bats. The auditor's response to the risk of material misstatement will vary accordingly.

2. Control risk

The risk that a misstatement that could occur in an assertion about a class of transaction, account balance or disclosure that could be material, individually or when aggregated with other misstatements, will not be prevented or detected and corrected on a timely basis, by the entity's internal controls. Control risk is perhaps easier to understand than inherent risk. Simply stated, if the internal control system does not do its job, there is a strong possibility that misstatement of which the auditor may not be aware, will occur.

Control risk is a function of the effectiveness of the design and operation of internal control in achieving its objectives but because of the limitations of internal control itself, it is very unlikely that a client's system will be perfect. Hence some control risk will exist. ISA 315 (Revised) states that "no matter how effective, internal control can provide an entity with only reasonable assurance about achieving the entity's financial reporting objectives". The likelihood of achievement is affected by ***limitations inherent to internal control***.

These limitations may be described as follows:

* management's usual requirement that the cost of an internal control does not exceed the expected benefits to be derived (cost/benefit). Control may be sacrificed due to the cost of implementing the control, thus increasing the risk that misstatement goes undetected. This is particularly so for smaller companies.

* most internal controls tend to be directed at routine transactions rather than non-routine transactions (Non routine transactions may bypass controls, resulting in misstatement).

* the potential for human error due to carelessness, distraction, mistakes of judgement and the misunderstanding of instructions.

* the possibility of circumvention of internal controls through the collusion of a member of management or an employee, with parties inside or outside the entity.

* the possibility that a person responsible for exercising an internal control could abuse that responsibility, for example, a member of management overriding an internal control.

* the possibility that procedures may become inadequate due to changes in conditions, and compliance with control procedures may deteriorate (for example, internal controls cannot handle a huge increase in sales).

It is not sufficient for the auditor simply to identify the presence of weaknesses in a client's internal control system, the important exercise is evaluating the effect which the identified weaknesses may have on the financial statement assertions. To illustrate; your client, a wholesaler, routinely sells its products to retailers on credit. The internal controls for credit sales are sound. However, over time, the practice of selling to staff members and street hawkers for cash has crept in without adequate internal control activities being formalised. For example, no specific cash sale documentation has been developed, cash is not adequately recorded and regularly banked, and there is no segregation of duties between recording sales and banking of cash. What assertions may be affected? The obvious ones are ***completeness*** of sales (are all sales being accounted for?) and ***completeness*** of bank/cash on hand (is all the cash received being accounted for?). Perhaps a less obvious assertion at risk is the ***completeness*** assertion for liabilities. If sales are not being accounted for, profits will be misstated and hence the liability to SARS for taxation will be understated.

3. Detection risk

The risk that the procedures performed by the auditor to reduce audit risk to an acceptably low level will not detect a misstatement that exists and that could be material, individually or when aggregated with other misstatements.

Detection risk relates to the nature, timing and extent of the auditor's procedures put in place to respond to the risk of material misstatement and reduce audit risk to an acceptable level. Detection risk is a function of the effectiveness of an audit procedure and its application by the auditor, and may arise because the auditor

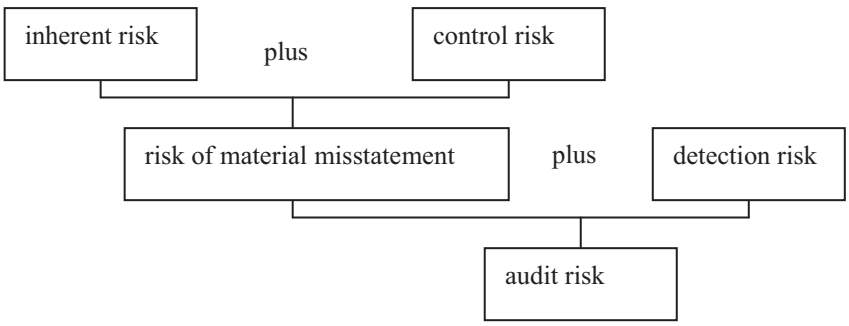
* selects an inappropriate audit procedure and/or
* misapplies an appropriate procedure and/or
* misinterprets the results of the test

Reducing detection risk is best achieved by complying with the relevant ISAs, particularly by

* sound planning
* proper assignment of personnel to the engagement team,
* the application of an appropriate level of professional scepticism and
* proper supervision and review of the audit work performed.

4. Relationships between audit risk, inherent risk, control and detection risk and material misstatement

* ***audit risk and the risk of material misstatement are not the same thing.*** Diagrammatically we can illustrate the difference as follows:



* ***the risk of material misstatement is made up of inherent risk and control risk***, e.g. the risk of material misstatement will be highest where there is a high level of inherent risk relating to the assertion and controls are weak. If controls are very strong (i.e. low control risk) and there is low inherent risk relating to the assertion then the risk of material misstatement relating to that assertion will be low.

* ***audit risk is a function of the risk of material misstatement and detection risk***, e.g. if there is a high risk of material misstatement and the auditor does not respond with effective selection and application of audit procedures, the risk of expressing an inappropriate audit opinion (audit risk) will be very high. In other words, to keep audit risk to an acceptable level, the auditor must ensure that detection risk is kept to a low level by sound planning, proper assignment of personnel to the audit team, proper supervision, etc.

Think of it another way. If you evaluate inherent risk and control risk at your client as high, it means that there is a strong possibility of material misstatement being present in the financial statements. As the auditor, you must minimise the chance of expressing an inappropriate opinion on the financial statements, in other words, you must reduce this risk (audit risk) to an acceptable level. How do you do that? The answer is by adopting an appropriate audit strategy and plan and assigning the right staff to the audit team (experienced and competent), having the audit team exercise professional scepticism and putting in place proper supervision and review procedures - ***by doing these things you will be reducing the risk of failing to detect the misstatements which you expect*** (due to the high inherent and control risk) ***to an acceptable level***. As the auditor, you have no control over inherent risk or control risk, inherent risk is "built in" risk and internal control is the responsibility of management. All you can do is to respond to these risks by reducing detection risk. Unlike inherent and control risk, detection risk is ***controllable*** by the auditor.

UNDERSTANDING THE ENTITY AND ITS ENVIRONMENT

INTRODUCTION

As you will know by now, the objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error at the financial statement and assertion levels, ***through understanding the entity and its environment***, including the entity's internal control, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement. The key to this is that unless the auditor has a thorough understanding of his client's business and the environment in which it operates, a proper identification and assessment of the risk of material misstatement is not possible. Simple examples illustrate this. If we don't understand how a company's manufacturing process works, what raw materials or components make up its products and how it identifies and records production overheads, how can we as auditors, identify and assess the risks relating to such account headings as finished goods inventory, work-in-progress, etc? How will we know if overheads are being appropriately included in the cost of inventory? If we are not familiar with the company's leasing policies, how will we determine whether leases should be treated as finance or operating leases? The examples are endless and the message should be clear – without a thorough understanding of the client, a substandard audit will be conducted.

Although "understanding the entity" is a clearly defined activity within the audit process, it is not a "once off, stand alone" activity. Knowledge about a client is acquired as the relationship with the client evolves. Each audit provides a better understanding of what we already know and new information about changes and developments in the business is added. Understanding the entity is dynamic, not static. It is not an exact science and there is no hard and fast set of procedures to be followed.

According to ISA 315 (Revised) – Identifying and assessing the risks of material misstatement through understanding the entity and its environment, an understanding of the entity establishes a frame of reference within which the auditor plans the audit and exercises professional judgement, for example when:

* assessing risks of material misstatement of the financial statements
* determining materiality
* considering the appropriateness of the selection and application of accounting policies and the adequacy of disclosures
* identifying areas where special audit consideration may be necessary e.g. the audit of related party transactions

* developing expectations for use when performing analytical procedures
* responding to the assessed risk of material misstatement, including performing further audit procedures, to obtain sufficient, appropriate evidence and
* evaluating the sufficiency and appropriateness of audit evidence obtained.

All of the above are fundamental to performing the audit but cannot be achieved without the auditor having a thorough understanding of the entity.

RISK ASSESSMENT PROCEDURES AND RELATED ACTIVITIES

Risk assessment procedures are those procedures carried out by the auditor to gather information about the client so that the identification and assessment of risks of material misstatement at the financial statement and assertions level can take place. Once this has been done, the auditor will have a basis for designing and implementing responses to the assessed risks of material misstatement.

Useful information about a client can come from any number of sources but will generally flow from the following:

1. Client acceptance of continuance procedures

Remember that by the time risk assessment procedures take place, the audit engagement will have been accepted and that prior to acceptance, a fair amount of information about the client would have been obtained. For example, information about the integrity of the directors would have been sought, discussions with the audit committee (if there was one) would have been held, and information about the size and complexity of the entity would have been gathered. In the case of an existing client, any major changes or developments would have been considered in making the decision as to whether to retain the client. The point is that some of the information gathered will be useful in identifying and assessing the risk of material misstatement.

2. Previous experience with the entity

Where the audit firm has been engaged by the entity before, there will already be a "store" of information about the entity. The extent of this information will depend on the previous engagements. If the firm has conducted the audit for a number of years then there is likely to be a good base of information. If the previous experience with the entity was, say, providing tax advice, then information relevant to an audit is likely to be far less. Clearly the auditor would need to determine whether information obtained in a prior period remains relevant.

3. Inquiries of management and others

Discussion with the client's personnel will perhaps provide the most information and the following examples serve to illustrate the diversity of employees and others who may be consulted.

* ***production personnel*** can provide information about the company's raw materials, finished goods, manufacturing process, etc

* ***marketing and sales personnel*** can provide information about the company's marketing strategies, products, competitors, etc

* ***human resource personnel*** can provide information about organizational structures, remuneration policies, labour disputes, etc

* ***internal audit personnel*** can provide information on investigations and assessments they have done as well as their evaluation of the company's own risk assessment procedures, etc

* ***financial and accounting personnel*** will be a major source of financial reporting information, including the accounting policies used, related parties, procedures for setting estimates, making provisions and establishing fair values, taxation, etc

* ***the company secretary, the company's legal counsel*** will be able to supply information about litigation, laws and regulations relevant to the company, important contractual obligations, etc

* ***the board of directors (those charged with governance)*** will provide information on the company's overall strategies etc, and will give the auditor a sense of the control environment at the company

* ***IT personnel*** will be able to provide important information about the company's computer system, etc

* ***an audit committee and risk committee*** will also provide information relating to accounting policies, internal control, financial reporting objectives (audit committee) and the company's own risk assessment procedures and policies regarding risk (risk committee)

* where applicable, ***the previous auditor*** may provide information pertaining to the previous audits, including audit problems and their resolution, dealings with the audit committee and board members, the competence of senior financial personnel and the control environment, etc. (Note: much of this information may have been obtained when the pre-acceptance procedures were carried out, but there is nothing to stop further contact with the previous auditor, provided the client gives permission.)

4. Observation

The observation of "what's going on" can provide a useful backdrop for understanding the client's operations. For example:

* a guided tour of a company's manufacturing plant will give the auditor a basic understanding of the production process. This understanding will put the audit of plant and equipment, work in progress, the allocation of production overheads, etc into context

* a tour of the company's business premises, IT centre, warehousing facilities, will also contribute to a better understanding of the client.

5. Inspection

Along with enquiry, ***inspection*** will be a major provider of information in gaining an understanding of the entity. At this stage of the audit, we are ***not*** carrying out a detailed inspection of "everyday" documents such as sales invoices or purchase orders on which we may conduct further audit procedures (substantive tests of detail). This is more likely to be a detailed review of the following kinds of documents

* business plans and strategies

* internal control procedure manuals, flow charts, organsational charts

* management reports, minutes of board meetings and board committee meetings

* the company's integrated report and prior year financial statements

* relevant trade and financial journals and internet sites

* important contracts

6. Analytical procedures

Analytical procedures carried out at this stage of the audit process may be useful in providing an overall indication as to whether the company's financial performance is as expected, but may produce results that are unexpected and which need to be explained. Ratio and trend analysis, including comparisons to prior periods, industry averages or between similar sections or divisions, may reveal unusual or unexpected relationships. The explanation may indicate the presence of material misstatement. For example, (there are any number of examples)

* there may be an increase in sales but a decline in gross profit

* debtors' ratios may have declined without credit policies having been changed

* sales commissions paid may have increased but sales may have declined.

7. Discussion among the audit team

This really amounts to the "two heads are better than one" principle. The discussion is an opportunity for

* the experienced members of the audit team to share their insights and knowledge of the entity and

* explain how and where the financial statements may be susceptible to material misstatement and for

* the new members of the team to inject fresh insight and question conventional thinking about the audit.

8. Gaining the required understanding of the entity and its environment, including the entity's internal control

In terms of ISA 315 (Revised) the auditor must obtain an understanding of

* ***the entity and its environment***

  ISA 315 (Revised) provides a basic framework as to what information should be gathered. This has been used as a basis for the charts and narratives which follow:

  - relevant industry, regulatory and other external factors
  - the nature of the entity
  - the entity's selection and application of accounting policies
  - the entity's objectives and strategies and related business risk
  - measurement and review of the entity's financial performance.

* ***the entity's internal control***

  Again ISA 315 (Revised) provides a useful framework the auditor can adopt to obtain this understanding. It suggests that the auditor should obtain an understanding of each of the following components of internal control

  - the control environment
  - the entity's assessment process
  - the information system including the related business processes relevant to financial reporting
  - control activities relevant to the audit e.g. general controls and application controls
  - monitoring controls.

Remember that the auditor is putting together a body of information which will enable the audit team to identify and assess the risk of material misstatement at financial statement level and at assertion level.

THE ENTITY AND ITS ENVIRONMENT

1. Industry, regulatory and other external factors

Factor	*Matters to consider*
Industry	* cyclical or seasonal * risk profile • high risk, e.g. fashion, technology • competition (demand, capacity and price) • labour volatility • size and market share within the industry • boom or recession * energy supply and cost
Regulatory	* accounting principles and industry specific practices * legal and regulatory framework • taxation, e.g. farming company • foreign transactions • operations, e.g. health regulations, consumer protection • environmental, e.g. pollution control • safety and security e.g. in the workplace * government policy • industry specific financial incentives • trade restrictions and tariffs • foreign exchange

2. The nature of the entity

Factor	*Matters to consider*
The entity : products, markets, suppliers and operations	* nature of business, e.g. retailer * stages and methods of production * outsourcing activities * geographic location of all facilities, e.g. head office, factories * labour and employment • unions • pension commitments • stock options and incentives • regulated, e.g. minimum wages * products and markets and revenue sources • key customers and suppliers • export/import • market share • pricing policies and margins * inventory locations, quantities and types * franchises, licenses and patents * research and development * internet trading * related parties

Factor	*Matters to consider*
The entity : ownership and governance	* structures • corporate e.g. subsidiaries, divisions • organizational, e.g. head office, regional offices • capital, e.g. classes and types of shares • listed * black economic empowerment * management philosophy * board of directors • adherence to corporate governance (King III) • risk management • reputations of members of the Board • meetings, e.g. full board, committees • committees, e.g. audit, nominations, social and ethics * operating management • capabilities • stability • key personnel • methods of remuneration, e.g. performance based • pressures to perform or meet deadlines * internal audit
The entity : investments and financing activities	* acquisition, mergers etc (executed or planned) * investments • other entities – joint ventures, partnerships • plant and equipment • technology * sources of finance * group structure e.g. subsidiaries * debt structure • covenants • restrictions • off balance sheet financing • leasing • related parties • derivatives
The entity: financial reporting	* the reporting environment • accounting principles and industry specific practices • deadlines • profit share or remuneration based on financials • reliance by 3rd parties • pressure from holding companies or overseas affiliates to perform • expectations of shareholders * specifically relevant accounting practices • revenue recognition • accounting for fair values • foreign currency assets, liabilities and transactions • accounting for unusual or complex transactions

3. The entity's selection and application of accounting policies

The auditor will need to consider whether the accounting policies selected by the client are

* appropriate for the business
* consistent with the financial reporting standards relevant to the industry.

If the policies adopted do not satisfy the above, the risk of material misstatement is increased. Of specific interest to the auditor, will be

* how the client accounts for unusual transactions
* the policies adopted for controversial or "new" issues for which there is no standard
* the reasons and appropriateness of changes the client has made to accounting policies
* how the client adopts and implements standards and regulations which are new to the company e.g. the client introduces a customer loyalty programme during the financial year and must implement the necessary financial reporting requirements.

4. The entity's objectives and strategies and the related business risk arising from these objectives and strategies

A business sets itself objectives and then puts in strategies to achieve these objectives. "Business risk" is the term used to describe those conditions, events, circumstances, actions or inactions which threaten the company's achievement of the objectives it has set and its ability to achieve those objectives. Business risk is broader than the risk of material misstatement of the financial statements; in other words, business risk includes risks other than the risk of material misstatement. Many of the business risks may increase the risk of material misstatement in the financial statements. The auditor must therefore be familiar with the client's objectives and strategies and evaluate whether they will increase the risk of material misstatement. Consider the following (simplified) examples :

Example 1

Objective :	Wearit (Pty) Ltd wishes to increase its market share
Strategy :	Increase sales by making the terms and conditions for granting credit to customers much less strict
Business risk :	making sales on credit to customers who will not pay
Potential material misstatement :	understatement of the allowance for bad debts, resulting in an overstatement of accounts receivable

Example 2

Objective :	Pills (Pty) Ltd wants to expand its health products business into the sports market
Strategy :	Import top quality, patented muscle growth and related products and advertise extensively
Business risk:	increased product liability, overestimation of demand, import regulation contraventions, e.g. on foodstuffs
Potential material misstatement :	underprovision for legal claims, overstatement of inventory value (no demand, or goods cannot be legally sold)

There are any number of business risks, the key is to have experienced audit team members who can identify them and evaluate whether they will give rise to material misstatement.

5. Measurement and review of the entity's financial performance

The auditor should obtain an understanding of the manner in which the performance of the entity and its management is measured. Measuring performance creates pressure on individuals and failure to perform can have serious consequences. Professional scepticism suggests that one way of avoiding negative consequences may be for management to manipulate the financial statements to present a better position than actually exists. For example, the directors of a subsidiary may stand to lose their jobs if the subsidiary does not meet certain turnover or profit targets for the financial year. This gives the directors the incentive (creates pressure) to manipulate the financial statements. This could be done by manipulating sales cut-off (including post year end sales in the year end sales figure), introducing fictitious sales with related parties, and manipulating costs to increase profits.

In effect, the auditor needs to consider the extent to which the entity's measurement and review system is likely to increase the risk of material misstatement of the financial statements. A further example may confirm your understanding of this. A series of performance measures are built into the directors' and managements' employment contracts, which directly affect their personal remuneration. Many of

the measures are based on the financial performance of the entity and thus present a real incentive for manipulation of the financial statements and other financial information. The auditor must understand the performance measurement exercise and must consider carefully which account headings (and related assertions) are susceptible to manipulation.

Some examples of information used by management for measuring and reviewing financial performance and which the auditor should consider include

* key performance ratios and indicators, trends etc including financial and non-financial information
* period-on-period financial performance analysis
* budgets, forecasts and variance analysis
* employee performance measures and "bonus" policies.

THE ENTITY'S INTERNAL CONTROL

In chapter 5 we discussed internal control in some depth and noted that a good way of gaining an understanding of an entity's internal control is to consider its five components separately and collectively. As indicated earlier ISA 315 (Revised) in fact recommends that this is how the auditor should go about obtaining the necessary knowledge of the system. Remember that ***an understanding of a client's internal control assists the auditor in identifying types of potential misstatement and factors that affect the risks of material misstatement, and in designing the nature, timing and extent of further audit procedures.***

Some of the aspects of internal control which were covered in chapter 5 have been repeated here, but as the client's internal control is so important to the auditor, the repetition is acceptable. Computerised systems, which contain a mix of manual and automated (programmed) controls are the norm and therefore very common in business. Obviously the degree, complexity and sophistication of computerised systems vary considerably, but in most cases the auditor will need to obtain a sound understanding of the role played by computerization in the company's internal control, particularly in relation to the information system and control activity components of the internal control process.

1. Component : the control environment

The control environment sets the tone of the organization and influences the control consciousness of its staff. It concerns the attitude and awareness of the directors and managers to internal control and its importance to the entity. The directors and managers should, by their actions and behaviour, promote an environment in which adherence to controls is regarded as very important. If managers set a bad example, ignoring controls and generally projecting a "slack" attitude, employees will soon adopt the same attitude. For example, a creditors clerk whose function it is to reconcile the creditors ledger accounts to the creditors statements, and then take the reconciliation to the financial accountant to be checked before payment is made, will soon not bother to reconcile properly, if at all, if he knows that the financial accountant does not check the reconciliation before authorizing the payment.

A good control environment will be characterized by

* communication and enforcement of integrity and ethical values throughout the organization
* a commitment by management to competent performance throughout the organization
* a positive influence generated by those charged with governance of the entity, e.g. non-executive directors, the chairperson (i.e. do these individuals display integrity and ethical commitment, are they independent, and are their actions and decisions appropriate?)
* a management philosophy and operating style which encompasses leadership, sound judgement, ethical behaviour, etc
* an organizational structure which provides a clear framework within which proper planning, execution, control and review can take place
* policies, procedures and an organizational structure which clearly define authority, responsibility and reporting relationships throughout the entity

* sound human resource policies and practices which result in the employment of competent ethical staff, provide training and development as well as fair compensation and benefits, promotion opportunities etc.

Gathering of evidence relating to the control environment can be achieved by ***observation*** of management and employees "in action", including how they interact, ***inquiry*** of management and employees, e.g. union officials, and ***inspection*** of documents, e.g. codes of conduct, organograms, staff communications, records of dismissals, minutes of disciplinary hearings etc. Obviously as the client/auditor relationship develops over time, it will become easier to understand and evaluate the control environment.

Generally a strong control environment will be a positive factor when the auditor assesses the risk of material misstatements. For example the risk of fraud may be significantly reduced. A poor control environment, or elements of the control environment which are poor, will have the opposite effect, e.g. the company may have excellent human resource policies, but may lack leadership and organizational skills. Employees may be competent but management may have a "slack" attitude towards controls.

2. Component : the entity's risk assessment process

This is the process which the company has in place for, inter alia,

* identifying business risks relevant to financial reporting objectives
* estimating the significance of each risk
* assessing the likelihood of its occurrence
* responding to the risk (taking action to address the risk)

This process of risk assessment may be formal or informal. Larger organizations are more likely to have a formal plan, e.g. specific committees who hold regular meetings, the appointment of a Chief Risk Officer and/or a Compliance Officer, but generally risk assessment is part of "managing". In doing their jobs, managers will identify and respond to risk.

Information about the client's risk assessment process will be gathered mainly by ***inquiry***, e.g. Risk Officer, Compliance Officer, Chief Executive Officer, and ***inspection*** of documentation where it is available, e.g. minutes of designated committee meetings, inter-office memo's on rectifying problems (responding to risk). An effective risk assessment process is advantageous for the auditor because the results produced by the in-house process provide the auditor with a platform to work from in assessing risk.

In terms of King III ***internal audit*** should primarily be risk based which means that the internal audit section is expected to carry out assessments and evaluations of the company's risk process and the company's response to risk. Internal audit will therefore be a good source of information for the external auditor when evaluating the client's risk assessment process.

3. Component : the information system

The auditor is required to obtain an understanding of the information system relevant to financial reporting and communication. The accounting system is part of the information system. Bear in mind that the client's information system will produce information which is not relevant to financial reporting. For example, the information system of a motor manufacturer may produce extensive information about sales to assist the marketing department, e.g. most popular colours, sales by dealer, month, geographical location, age of purchaser, etc. Whilst this may be interesting to the auditor (and sometimes helpful, e.g. it may provide some evidence of the saleability of inventory), it is not directly related to financial reporting. The auditor must obtain a thorough understanding of

* the classes of transactions in the client's operations that are significant to the financial statements, e.g. sales, wages
* the procedures within both IT and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in the financial statements

* the related accounting records, supporting information and specific accounts in the financial statements in respect of initiating, recording, processing and reporting transactions

* how the information system captures events and conditions, other than transactions that are significant to the financial statements, e.g. contingent liabilities

* the financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures

* controls over the passing of non-standard journal entries used to record non-recurring, unusual transactions or adjustments

* the manner in which financial information is conveyed to management, the Board, the audit committee and external bodies, e.g. the JSE in the case of a listed company.

The chart below provides a breakdown of matters which the auditor might consider when obtaining information about a ***computerised*** information system.

Factor	***Matters to consider***
computerised applications	* which applications are computerised,e.g. • payroll – not computerised • acquisitions and payments – computerised * computer environment • micro, network, centralised • use of bureau (see chapter 8 for a discussion on computer environments) * the application software • purchased or in-house software • key processing functions • nature and source of inputs • output produced • important masterfiles and tables • interface between applications • new or established
hardware	* makes and capacities of CPU's, drives, printers, servers, terminals (important for establishing compatibility with the auditors hardware and software and for understanding the system) * physical location (branches , factory, etc)
software	* details of all software which is used for managing the functions of the hardware and data • operating systems • database management systems • utilities • access control software • programme change control software
organization and control	* general and application controls (Chapter 8) * communication and reporting lines * IT personnel and their job descriptions * steering committee details * internal audit involvement in IT
complexities of the system	* the presence of: • networks (LANS, WANS) • electronic data interchange (EDI) • electronic funds transfer (EFT) • real time systems • the Internet • high levels of system integration • complex databases, communication networks
the level of dependence (of the client on its normal system)	* degree of disruption which would occur if the system was not functional for a lengthy period * the dependence of a particular functional area on timely, accurate computing, e.g. wages in a large labour intensive industry

The auditor should be mindful that computerised (IT) systems pose specific risks to an entity's internal control. These risks include the following:

* a computer will process what is input and will do so in the manner in which it is programmed. If for example there is an error in programming, that error will be repeated every time the relevant transaction is processed, e.g. a programming error results in the VAT on sales being calculated on the selling price plus VAT e.g. 14% of 114%. If 5000 invoices are processed the computer will make the mistake 5000 times.

* unauthorized access to data can result in instant and huge destruction or contamination of data e.g. deletion of the debtors masterfile.

* IT personnel gaining access privileges they should not have, resulting in a breakdown of segregation of duties e.g. a systems analysts gains access to the salaries masterfile and alters his salary.

* unauthorised changes to data in masterfiles, systems or programmes.

* processing of fraudulent transactions instantaneously e.g. unauthorized electronic funds transfer which almost instantaneously moves money out of the company's bank account.

* potential denial of access to electronic data e.g. employees/customers cannot get into the database because of system failure.

The auditor should also be mindful that the information system as a whole, or elements of it, can be placed at risk, by for example

* ***new employees*** who have a different understanding of, or attitude to internal control, e.g. a newly appointed IT manager has a less strict attitude to access controls than his predecessor

* ***rapid growth*** in the company which places severe strain on the controls, e.g. a significant increase in the demand for the company's products has resulted in the company letting its credit-worthiness checks lapse (so as not to lose sales) due to a lack of time and staff to carry out the checks. Automated (programmed) controls relating to creditworthiness may be overridden permanently or disabled

* ***new technology*** which can lead to disruption of internal controls – introducing a network system may result in data being lost or corrupted or existing controls becoming inappropriate

* ***introducing new business models*** which may result in the existing internal controls being rendered inadequate, e.g. introducing sales over the Internet to a long established (physical) retail business may introduce problems in controls over banking, receipt and dispatch of goods, etc

* ***corporate restructuring*** which may result in staff reductions, new lines of authority etc, thereby jeopardizing for example, division of duties and authorization controls

The auditor will have to carefully assess whether and how the changes affect the internal control objectives and the potential for material misstatement.

Details of the information system (including the accounting system) can be gathered by

* ***inspection*** (or creation) of flowcharts of the system, user manuals etc.

* ***observation*** of the system in action, e.g. what happens when goods are delivered by a supplier, what documents are called up on screen, what access controls are in place

* ***inquiry*** of client staff and the completion of internal control questionnaires

* ***discussions*** with prior year audit staff, management and possibly outsiders, e.g. application software suppliers

* ***discussions*** with internal audit staff and ***review*** of internal audit workpapers

* inspection of exception reports, error reports, activity reports produced by the system

* ***tracing*** transactions through the information system, sometimes called "walk through" tests.

4. Component : control activities

This component was covered extensively in chapter 5, and is also covered in chapter 8.
Control activities are the policies and procedures that are implemented to ensure that management's objectives are carried out. Not all control activities relate to financial reporting and the auditor will concern himself only with those that relate to areas where material misstatement is more likely to occur. Control activities essentially include such things as

* authorization of transactions (which is a form of isolating responsibility)

* segregation of duties, e.g. separating custody of inventory from keeping of inventory records

* physical control over assets, e.g. restricting access to the warehouse

* comparison and reconciliation, e.g. reconciling the bank account monthly

* access controls, e.g. access tables, user profiles, Ids and passwords in a computerized environment

* custody controls over blank/unused documents, e.g. order forms, credit notes

* good document design (to achieve accuracy and completeness of information)

* sound general and application controls in IT systems (see Chapters 8 and 9)

Information about control activities will usually be gathered in the same way as information about the information system as a whole is gathered, e.g. ***inspection*** of control procedure manuals, ***observation*** of controls in action, ***inquiry*** of employees as to the procedures they carry out and the completion of internal control questionnaires.

5. Component – monitoring of controls

You will recall that, at the outset, management identifies the objectives which the company's internal control process should achieve both overall and right down to transactions level. Monitoring of the system tells management how well the internal control process is doing ***over time***. Management (and the board) wish to know if controls are operating as intended and monitoring assists in providing this information. Some procedures which are described and carried out as control activities are a form of monitoring e.g. a senior accountant inspects the monthly bank reconciliation carried out by his assistant to ensure that it has been done and done correctly. Monitoring as a component of the internal control process looks at ***all of the components of the process*** not only at the control activity component. For example, management's monitoring of disciplinary actions and warnings to employees relating to breaches of the company's "code of conduct" may indicate a decline in the control environment, and the ongoing monitoring of the company's poor performance on contracts may reveal that the risk assessment component is not effective.

In larger companies, internal audit departments usually contribute to the effective monitoring of control activities, and the external auditor will frequently rely on work carried out by the internal auditor. Monitoring will often take place at a subsequent stage, e.g. the manager of a telesales system playing back recorded sales transactions to confirm that telesales operators are "following the rules", or the scrutiny of activity logs/exception reports by the IT manager on a weekly basis. Information from outside the company can also provide meaningful insights into whether the "system is working", e.g. monitoring complaints from customers will often give a good indication of aspects of the business which are not functioning as required. Monitoring the number of bad debts over time, gives an indication of whether creditworthiness checks are effective.

Information about monitoring can be obtained by the auditor by ***inquiry*** of management and staff, working with internal audit and ***inspecting*** documentation relating to a monitoring process or performance reviews.

SIGNIFICANT RISKS

1. On its initial release in 2004, ISA 315 introduced the concept of significant risks and defined them as risks that require ***special audit consideration.*** Some guidance is given on what the auditor might consider in deciding whether a risk is significant or not, but no guidance is given on what special audit considerations might be. However, there is nothing to worry about here, as the process remains the same. In terms of ISA 315 (Revised), the auditor is required to carry out procedures to identify and assess the risk of material misstatement at financial statement and at assertion level ***and*** as part of the assessment process, decide whether any of the risks identified are significant. The assessment of risk is really an exercise in grading the risks identified. In practice risks are often graded as low, medium or high, but however the risk is graded, the auditor must respond appropriately. This is the key. For example, the risk relating to the valuation of a jewellery business inventory of diamonds is probably going to be regarded as high or ***significant***. As discussed earlier, auditors will probably not know one diamond from the next and will not be able to judge its clarity, cut or carats to determine whether it has been fairly valued. Whether the auditor calls it a high risk or significant risk, he has assessed the risk of material misstatement in the inventory account heading as very likely and his response, in this case, is likely to involve making use of an expert. The further audit procedures (response to risk) will involve making use of an independent expert. Essentially what is important is that the auditor identifies comprehensively the risks of material misstatement and responds accordingly, not whether the classification of the risk is "correct".

2. In assessing the severity of the risk, i.e. whether the risk is a significant risk, the auditor must consider

2.1 Whether it is a risk of fraud: i.e. if the auditor considers that there is a risk of fraudulent manipulation of the financial statements, it would be a significant risk.

2.2 Whether the risk is related to recent significant economic, accounting or other developments, i.e. the suggestion here is that where there are new conditions at a client which the auditor considers may give rise to a risk of material misstatement, the risk should be regarded as significant because the condition is new. For example, a company finds itself in severe financial problems for the first time in its history, to the extent that its going concern activity is seriously threatened. This would be a significant risk.

2.3 The complexity of the transactions (giving rise to the identified risk). For example, the audit client commences trading in derivatives and the auditor considers that there is a risk of material misstatement arising from the inappropriate application of the financial reporting standards relating to derivatives. Due to the complexity of derivative transactions ***and*** the fact that trading in derivatives is new to the company, this would be regarded as a significant risk.

2.4 Whether the risk involves significant transactions with related parties. Because of the potential for non-arms-length transactions occurring between the company and related parties, there is always a risk of material misstatement of related party transactions and where such transactions are material and frequent, the risk should be regarded as significant.

2.5 The degree of subjectivity in the measurement of the financial information related to the risk. The greater the subjectivity, the more likely the risk will be significant. For example, the valuation of plant and equipment for a large manufacturing company which has to account for numerous and varied impairments of its plant and equipment at year end, will probably present a significant risk.

2.6 Whether the risk involves significant transactions that are outside the normal course of the business, or otherwise appear unusual due to their size or nature. These types of transactions are unlikely to be subject to the normal, everyday routine control activities associated with the company's transactions and therefore may well result in material misstatement. Material loans to directors or sale of some of the company's manufacturing equipment might be regarded as significant.

Remember that the reason for identifying and assessing the risk is so that the auditor can determine the nature, timing and extent of further audit procedures. Grading the risks helps fine tune the audit plan and respond appropriately. Before the actual determination of the response, the auditor will obtain an understanding of the company's controls relevant to the risk identified, as the company's controls will affect the auditor's response. For example, if management recognizes the risk of material misstatement

arising from related party transactions, they may have already implemented strict control activities over these transactions, e.g. additional authorization requirements, monthly reports to the board on all such transactions, and sound procedures for identifying related parties. From an audit perspective this is likely to reduce the "significance" of the risk associated with related party transactions, but of course, will not eliminate it.

3. There is no unique set of procedures which the auditor carries out to respond to significant risks. By definition, a significant risk is important and if it is inadequately addressed, could lead to material misstatement going undetected. It is logical therefore that the engagement partner would concentrate on

3.1 Getting the composition of the audit team right with regard to knowledge, experience and attitude (good level of professional scepticism).

3.2 Carefully evaluating the full effect of the significant risk ***and*** how it may manifest itself. For example, if the audit manager thinks that there is a significant risk that management may manipulate the financial statements, he should consider very thoroughly how this could be done. Fictitious sales, overstating inventory, making use of related parties etc are all methods of manipulating financial information, and the audit team will need to respond to all these methods.

3.3 All assertions affected should be identified and the ***best quality*** evidence should be sought by the audit team making use of normal audit procedures, e.g. inspection, confirmation, enquiry.

THE CONCEPT OF MATERIALITY

INTRODUCTION

Materiality is a fundamental concept in auditing. The objective of the audit is to express an opinion on whether the financial statements are fairly presented in all material respects. The audit report is a statement by the auditor that, in his opinion, the financial statements do not contain ***material*** misstatement. It is generally understood and accepted by users of financial statements, that the amounts reflected in the financial statements are not 100% accurate and that they may contain a margin of error or uncertainty. However, this margin of uncertainty must be acceptable to users otherwise the financial statements are of little value. Once the misstatement falls outside the acceptable margin it becomes ***material*** and is likely to affect the users' decisions.

There are two ISAs which relate to "materiality" in the context of the audit of financial statements
ISA 320 – Materiality in planning and performing an audit and
ISA 450 – Evaluation of misstatements identified during the audit.

ISA 320, as its title suggests, is concerned with materiality at the planning and performing stage of the audit, i.e. setting materiality levels to assist in the planning and performance of the audit, whilst ISA 450 is concerned with materiality as part of evaluating the effect of misstatements identified on the audit, and of uncorrected misstatements on the financial statements for the purposes of forming an opinion on fair presentation.

ISA 320 is a very general statement and is not particularly prescriptive. This is mainly because whilst an understanding of materiality in auditing is essential, the manner in which firms in practice implement the concept varies considerably. Essentially the statement presents the principles and leaves the rest up to the auditor.

In its discussion on materiality, ISA 320 explains that:

* misstatements, including omissions, are considered to be ***material*** if they, individually or in aggregate could reasonably ***be expected to influence the economic decisions*** of users taken on the basis of the financial statements

* judgements about materiality are made in the light of surrounding circumstances and are affected by the ***size*** or ***nature*** of a misstatement, or a combination of both

* judgements about matters that are material to users of the financial statements are based on a consideration of the common financial information needs of users ***not*** specific individual users

  A less formal explanation might be that a matter will be material if a user of financial statements should know about it when making a decision based on the financial statements.

The difficulty for the auditor is that he is required to decide what users of the financial statements as a group will regard as material in the context of fair presentation. Judgements about what is material to users of the financial statements are based on a consideration of the common financial information needs of users and not the needs of specific individuals. In making these judgements the auditor is entitled to assume the following:

* users have a reasonable knowledge of business and economic activities and accounting and a willingness to study the information in the financial statements with reasonable diligence

* users understand that financial statements are prepared, presented and audited to levels of materiality (i.e. users know financial statements are not 100% correct)

* users recognize the uncertainty in the measurement of amounts based on the use of estimates, judgements and the consideration of future events and that

* users make reasonable economic decisions on the basis of the information in the financial statements.

In terms of the IASB "Framework for the Preparation and Presentation of Financial Statements", financial statements which meet the needs of providers of risk capital to a company, will also meet the needs of most other users of the financial statements. This essentially means that in deciding on what is material to users, the auditor can assume that what is material to investors in the company will be material to other users.

THE NATURE OF MATERIALITY

1. Materiality is subjective

Ten auditors would probably come up with ten different decisions when setting a materiality level (i.e. the level of acceptable misstatement) at the planning stage, at the performance stage or deciding on whether a particular matter is material to fair presentation at the evaluating stage. It is not a defined concept, and professional judgement will play a large part in the decision. For example, if accounts receivable is reflected in the annual financial statements at R500 000, would an overstatement of R5 000 be material? R10 000? R20 000? R50 000? There is no definite answer. Of course the auditor does not decide on a materiality level by just choosing a nice round figure. Other factors will also have to be considered, for example, the size of the accounts receivable balance in relation to the current assets and total assets, as well as the profit or loss which has been made for the period. The auditor may be able to accept an overstatement of R50 000 in the accounts receivable balance itself, but if the overstatement is due to an understatement of the allowance for bad debts, then it will be necessary for the auditor to consider the misstatement in relation to the profit or loss made by the company as well. Remember that the auditor is having to make judgements about what users will consider to be an acceptable level of misstatement.

2. Materiality is relative

What is "material" will vary from user to user and from audit client to audit client. What is regarded as material for the financial statements of a medium sized company, may be totally insignificant to an international conglomerate, and a matter which is material to a private investor may be insignificant to a "unit trust" investor.

Because materiality is relative, it is necessary to establish bases against which it can be measured, e.g. a misstatement of R50 000 is material ***relative*** to net income of R500 000 but not material ***relative*** to net income of R5 000 000. We cannot say that R1 000 000 is material just because it is a large amount (to us!) because in the case of a large company it is simply not material. If a listed company's net profit is misstated by R1 000 000, users decisions are unlikely to be influenced.

Instead of just using a convenient pre-established amount, audit firms may use percentages of account headings or account groupings as a starting point or benchmark for setting the level, for example:

Account heading/grouping		%
Net profit before tax	:	5%
Current assets	:	5%
Current liabilities	:	3%
Total assets	:	3%
Turnover	:	1%

Note: this is only an illustrative example, other account headings/grouping may be used. Percentages may also vary and may also be presented as a range, e.g Turnover ½ to 1%. Benchmarks may also vary considerably from industry to industry. For example, benchmarks which may be appropriate for an audit at a supermarket company, may not be appropriate for a company which runs hospitals, as the relationships between account balances within the financial statements differ from industry to industry, e.g. supermarket company will have very high turnover and low profit margins, whilst hospital companies may have lower turnover but higher profit margins.

Perhaps the most important point to make here, is that the vast majority of misstatements affect the comprehensive statement of income and the statement of financial position but can be material to one and ***not*** to the other. For example, a company has total assets of R3 000 000 and net income before tax of R250 000. An error in the calculation of depreciation has resulted in an overstatement of fixed assets of R40 000. If the above percentages are used, this misstatement ***would not be*** material relative to the guideline for total assets (3% of R3m) but ***would be*** material relative to the guidelines for net profit before tax (5% of R250 000). It is for this reason that most auditing firms will use net income before tax as the base to measure the materiality of the misstatement, particularly in view of the fact that net income before tax is an important figure for most users.

It is interesting to note that ISA 320 recognises the use of benchmarks but does not prescribe any percentages to be used in setting materiality levels. This serves to emphasise the subjectivity surrounding the concept and the need to use professional judgement.

3. Materiality can be both quantitative and qualitative

An amount which is ***quantitatively*** material will be one which exceeds the amount which the auditor determines is material, i.e. the amount of misstatement which could influence the decisions of a user. For example, an overstatement in inventory of R100 000 may exceed the preset materiality level of R80 000. If this is the basis on which materiality is determined, it follows that an overstatement of R79 999 would not be material.

A matter which is ***qualitatively*** material will be one which is regarded as material when judged against a factor other than an amount. For example, important disclosure may be omitted from the financial statements. If this omission would influence a user, it becomes qualitatively material. Disclosure is not the only qualitative factor to be considered.

Both the quantitative and qualitative aspects of materiality should be considered by the auditor as a matter may be material in respect of one and not the other. For example, assume that the amount of misstatement the auditor can accept in the accounts receivable balance is R100 000. If the auditor discovers say, R90 000 of error in the balance arising from genuine mistakes, e.g. receipts from debtors inadvertently not accounted for or credit notes not passed, even if the errors were not corrected, the auditor would accept that the errors were ***quantitatively*** immaterial. If, however, the auditor identified misstatement of R90 000 arising from the deliberate inclusion of fictitious debtors in the account balance, the auditor would regard this as ***qualitatively*** material and would not accept it, despite the amount being below the R100 000 limit.

Another example might be that the auditor discovers an amount of R75 000 included in the accounts receivable balance, which is actually a loan to a director. Loans to a director attract disclosure

requirements and if these have not been met (which is likely in this situation), the misstatement of accounts receivable would be ***qualitatively*** material, although not ***quantitatively*** material.

PLANNING MATERIALITY and PERFORMANCE MATERIALITY

In terms of ISA 320, the concept of materiality is applied at the planning stage of the audit, (***planning materiality)*** during the performance of the audit (***performance materiality)***, and at the evaluating stage of the audit ***(final materiality)***. Final materiality is dealt with later in the chapter.

1. Planning materiality

When planning the audit the auditor makes judgements about the size of misstatements that will be considered material. Having an idea about the size of misstatement he is looking for, assists the auditor in

* determining the nature, timing and extent of risk assessment procedures
* identifying and assessing the risks of material misstatement
* determining the nature, timing and extent of further audit procedures.

Planning materiality is in a sense, an overall guideline to the audit and is the auditor's judgement as to the amount of misstatement a user can "live with".

1.1 Setting planning materiality levels

In terms of ISA 320, when establishing the overall audit strategy, the auditor is required to determine "materiality for the financial statements as a whole" and may also establish materiality levels to be applied to classes of transactions, account balances or disclosures. This means that in principle (and in practice) that there will be a planning materiality level set for the financial statements as a whole, and planning materiality levels (of a lesser amount) to be applied to classes of transactions, account balances and disclosures.

Setting planning materiality levels for the financial statements as a whole involves actually quantifying the amount of misstatement which the auditor believes could be present in the financial statements without affecting fair presentation. In the introduction to this chapter, we pointed out that financial statements are not 100% accurate and users understand that; but what is acceptable? 95% correct, 80% correct? Setting a materiality level attempts to quantify the level of misstatement which is acceptable. This is done so that the audit can be planned in such a manner that there is a reasonable chance of identifying misstatements which would exceed the acceptable level of misstatement. As a result, we might say that as an overall "guide" the financial statements could be out by R1 000 000 and still be fairly presented.

However, setting a planning materiality level at the overall financial statements level ***does not really mean a great deal***. This is because the audit is carried out on individual account balances and classes of transaction and disclosure, and this is the level at which the audit must be planned. The next step therefore, will be to consider the amount of misstatement which could be tolerated within an account heading before fair presentation of that account heading is lost. Setting planning materiality for classes of transactions and account headings is very subjective and requires significant professional judgement. Audit firms have different ways of approaching this but the principles remain the same, i.e. the auditor should consider what amount of misstatement each account heading can contain before it is no longer fairly presented. This decision will have a direct bearing on the ***extent*** of testing and may change the ***nature*** and ***timing*** of testing as well.

1.2 Factors which may be considered when quantifying planning materiality

Remember that the auditor is using his judgement to decide how much misstatement users of the financial statements would be prepared to accept knowing that the financial statements are a fair presentation and not a "100% correct" certification. The following factors may influence the auditor's thinking:

* ***the use of benchmarks*** - this is probably the most common starting point and was discussed under the nature of materiality point 2.

* ***importance of specific information to users*** – e.g. a bank has provided a long-term loan to the client. One of the terms/conditions of the loan is that the client must maintain a preset current ratio. If this is not achieved the loan must be repaid within six months. The auditor would regard current assets and current liabilities as having increased importance, as a user (the bank), will be specifically relying on the fair presentation of the amounts reflected under these account headings. The auditor would plan the audit so as to ensure that current assets and current liabilities are fairly presented.

* the ***key disclosures*** in relation to the industry in which the entity operates, e.g. research and development costs and disclosures in the pharmaceutical industry, or bonuses paid in the banking industry particularly in respect of directors. The auditor will want to be sure that these amounts and disclosures are as fairly presented as possible.

* ***legal requirements*** - the same logic will apply where financial information is governed by legal or regulatory requirements e.g. an amount or fact which must be specifically disclosed in terms of the Companies Act or an accounting standard or JSE regulations should be carefully and thoroughly audited to ensure that misstatement (quantitative or qualitative) is kept at an acceptable level. Users expect fair presentation of these amounts and disclosures as they are of specific interest.

* the opinions, views and expectation on materiality of ***those charged with governance and the audit committee***.

2. Performance materiality

Performance materiality levels will be set when the auditor performs tests on specific account balances or classes of transactions. (Ignore disclosure for the moment). Let's say that the auditor sets planning materiality for the audit of inventory at R100 000. Simplistically this means that the auditor is satisfied that fair presentation of inventory will still be achieved even if material misstatement of up to R100 000 in the inventory balance is not detected. So does this mean that when the auditor carries out the audit of inventory, his objective will be solely to detect errors which are individually over R100 000? The answer is no, for the following reason. The R100 000 planning materiality limit is the maximum or total amount of misstatement which the auditor considers is acceptable for inventory. If the auditor looks only for individual errors of R100 000 he will be overlooking the fact that the inventory balance could still be overstated by individual errors of less than R100 000 but which in aggregate (total) exceed R100 000, say R45 000, R70 000 and R13 000. Performance materiality is again a matter of professional judgement and is not a simple mechanical exercise. Because performance materiality levels are lower (stricter) than planning materiality levels, larger samples (extent of testing) will be tested. This is logical; in this example the auditor is not looking for individual errors exceeding R100 000 but rather for smaller errors which, when added together exceed R100 000.

2.1 In terms of ISA 320, the auditor must determine performance materiality for the purposes of

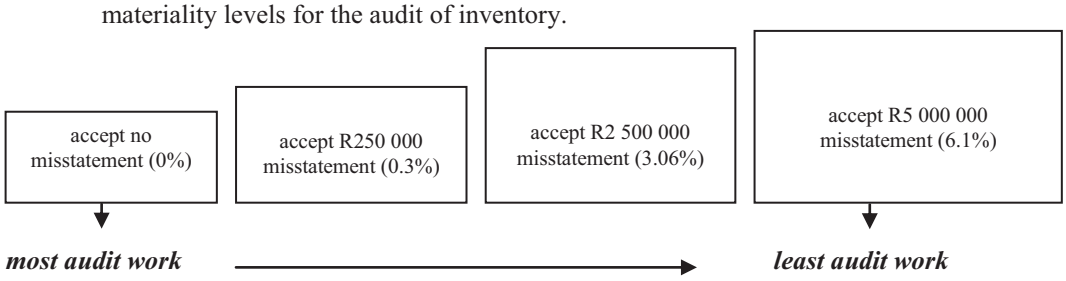
* assessing the risks of material misstatement (in the class of transactions, or account balance) and
* determining the nature, timing and extent of further audit procedures.

Again this is logical; if the auditor doesn't quantify what a material misstatement is, he won't know what he is looking for or how he should go about finding it!

Think about it like this; if you were told by your audit senior to identify and assess the risk of material statement occurring in the accounts receivable balance of R2 000 000, you would need to know, inter alia, what amount would be considered to be material. Are you considering the risk of misstatement of R5 000 or R500 000? The risk that the accounts receivable balance is "misstated" by R5 000 is probably very high, but the risk that it is misstated by R500 000 is probably very low. Similarly when you carry out the audit plan to respond to your risk assessment, the procedures that you would conduct to ensure that the probability that the aggregate of uncorrected and undetected misstatements does not exceed R5 000 is reduced to an appropriately low level, will be very different to those you would conduct if the materiality level was R500 000. Misstatements of R500 000 in a balance of R2 000 000 shouldn't be too difficult to find, but misstatements of R5 000 (in aggregate)

could require far more audit work. Obviously the materiality levels given in this example are rather ridiculous but they serve to illustrate the point!

2.2 As you will have gathered, the performance materiality level set will directly affect the nature, timing and extent of testing. Consider the following hypothetical example: The statement of financial position (balance sheet) of the Zed Company Ltd, a listed company reflects an inventory balance of R81 463 000. Let us assume a range of four possible planning materiality levels for the audit of inventory.



If users of The Zed Company Ltd's financial statements insisted that no amount of misstatement was acceptable in the inventory balance, we would have a materiality level of (zero) 0. To satisfy the users that there were no misstatements in inventory, we would have to count and price every single inventory item and ensure that every item was saleable at above cost, and in perfect condition. We would also have to ensure that every single item of inventory purchased or sold has been accounted for and so on. Of course this is a highly theoretical situation but it illustrates the point that the extent of audit work would be huge (extent), every kind of audit procedure would have to be used (nature) and we would take all year to do the audit (timing)! The cost of the audit would be astronomical. It is an impossible situation.

If the users had decided that they will accept R250 000 of misstatement, it follows that we could test less extensively. This is because that even if R250 000 of misstatement is present, but is not identified, users will not be concerned as misstatement of up to R250 000 is not going to influence their decisions. Based on this premise, if users had decided that R2 500 000 or R5 000 000 of misstatement was acceptable then we could test even less. The difficulty is that users don't conveniently inform the auditors of what amount of misstatement is acceptable, that's left to professional judgement!

Also, just a reminder; performance materiality levels take into account the fact that we test for misstatement which in aggregate might exceed the planning materiality level. Performance materiality will be a lower amount than planning materiality.

It doesn't end there; we must also remember that an error in inventory is not going to be confined to one account balance only and could result in material misstatement elsewhere in the financial statements, e.g. net profit before tax. To illustrate the point very clearly, The Zed Company Ltd made a net profit before tax of only R2 604 000 in the year 0002 (and a loss in year 0001), so a misstatement in inventory of R2 500 000 or R5 000 000 would have a really significant effect on net profit before tax and the financial statements as a whole, despite the fact that the misstatement is a small percentage of current and total assets. Expressed another way, a misstatement of R2 500 000 which affects both inventory and net profit before tax could ***not*** be regarded as ***immaterial*** as it has a significant effect on the company's profit despite being "not material" to the inventory balance.

3. Planning for qualitative misstatement.

Qualitative misstatement essentially deals with disclosure. Having obtained a thorough understanding of the entity and its environment before considering planning materiality, the auditor should have a good idea about disclosures which, if omitted or inadequately presented, could influence the decision of the user. For example:

* inadequate or improper descriptions of accounting policies which could mislead the user
* related party transactions
* directors remuneration
* litigation in which the client is involved or
* failure to disclose the possible cancellation of a manufacturing licence or the loss of a substantial market.

Alerted to the possibility of these qualitative misstatements, the auditor formulates the audit plan to address them. Some or all of the tools in the auditor's toolbox will be used to identify qualitative matters, e.g. inquiry, inspection. Experienced staff may be used to determine whether the qualitative misstatements have been appropriately dealt with.

4. Revision of planning and performance materiality levels.

Once a planning materiality level has been set, can it be changed as the audit progresses? The answer is yes. Planning materiality levels (whether for the financial statements as a whole or for a class of transactions or account balances) are based upon the auditor's initial understanding of the entity. If subsequent to setting planning materiality, further information comes to the auditor which would have affected the auditor's thinking about planning materiality, the auditor can if necessary, change the planning materiality levels. Remember that planning materiality is the auditor's "estimate" of what users of the financial statements would regard as the acceptable level of misstatement which could be present in the financial statements without influencing their decisions. If the auditor discovers something which would have affected his initial "estimate", he should change it. For example at the time of setting planning materiality, the auditor may not have known that strict debt covenants which require the company to satisfy a range of financial ratios if it wishes to retain the loan, had been added to the agreements with loan providers. This would warrant a change in the planning materiality levels initially set as the needs and expectations of (some) users (loan providers) will probably have changed. The margin of misstatement which they are prepared to accept in the account balances which affect the debt covenant ratios will have been reduced. Another example is as follows. During the course of the audit, long after having set planning materiality, the auditor discovers that the financial statements will be submitted to the Department of Trade and Industry from whom the audit client wishes to borrow money. Before they will advance a loan the DTI requires inter alia, that the company's AFS reflect certain profit, turnover and asset "levels". As the auditor now has knowledge of reliance by a user on specific balances in the financial statements, his estimate of planning materiality is likely to change. There is greater risk of misstatement in these balances because the client may be tempted to manipulate them to satisfy the "levels" required by the DTI.

Performance materiality directly influences the extent (and nature and timing) of the further audit procedures which are conducted by the audit team on a particular class of transactions or account balances. The auditor sets performance materiality to match his assessment of the risk of material misstatement in the class of transaction or account balance, so if the information comes to the auditor which changes his initial assessment of the risk of material misstatement, performance materiality may need to change. This will in turn, change the "further audit procedures" which must be performed to reduce audit risk to an acceptable level.

Finally, in practice, preliminary judgements about materiality may be based upon preliminary or draft figures. If this is the case the auditor will need to consider whether planning materiality will need to be adjusted if the client's final figures differ substantially from the draft figures.

MATERIALITY AT THE EVALUATING STAGE (FINAL MATERIALITY)

1. Introduction

ISA 450 – Evaluation of misstatements identified during the audit, provides guidance on how the auditor should proceed with regard to misstatements identified on the audit. The statement says that the auditor must

* evaluate the effect of identified misstatements ***on the audit*** and

* evaluate the effect of uncorrected misstatements if any, on the ***financial statements***.

Final materiality is the materiality level or guideline against which the auditor measures the effect of uncorrected misstatements on the financial statements.

2. Misstatements

* ISA 450 defines a misstatement as "a difference between the amount, classification, presentation or disclosure of a reported financial statement item and the amount, classification,

presentation or disclosure that is required for the item to be in accordance with the applicable accounting framework"

* misstatements (errors) may arise from
  - an inaccuracy in gathering or processing data
  - an omission of an amount or disclosure
  - an incorrect accounting estimate arising from overlooking, or clear misrepresentation of, facts
  - judgements of management concerning accounting estimates that the auditor considers unreasonable or the selection of accounting policies which the auditor considers inappropriate

* misstatements can arise from error (as described above) or from fraud, which is dealt with later in this chapter

* ISA 450 requires that the auditor accumulate (record) all misstatements identified on the audit unless they are clearly trivial. Clearly trivial should be taken to mean that the misstatement is very small, insignificant and inconsequential. Clearly trivial is not another phrase for not material; because a misstatement falls below the materiality level it is not automatically regarded as trivial

* uncorrected misstatements are misstatements which the auditor has accumulated during the audit but have not been corrected by the client.

3. Consideration of identified misstatements as the audit progresses

Essentially this requirement is about the auditor monitoring how the audit is going in respect of what the auditor expected and what is reflected by the materiality levels and audit strategy and plan which were put in place. If misstatements identified on the audit suggest that things are not going as expected or planned, the auditor may need to revise the audit strategy and plan. For example, the auditor conducts further audit procedures on the existence of inventory. If the number of instances where the existence of the inventory items is in question is beyond what is expected by the auditor, and the value of the (non-existent) items identified is material or may be approaching materiality, the auditor will need to consider whether the audit plan needs to be revised. The instances of non-existence identified, may suggest to the auditor that fraud has taken place or internal controls have broken down and that a revised plan to respond to these 'new" risks must be put in place. The auditor may choose to extend his own testing (and/or change the nature of testing) or request management to conduct the necessary tests to identify missing (non-existent) inventory.

4. Evaluating the effect of uncorrected misstatements on the financial statements

This is about making the final materiality decision – in other words, the auditor now has to decide what to do about any uncorrected misstatements. The auditor needs to judge whether the uncorrected misstatements are likely to influence the decision of a user. To understand final materiality we perhaps need to remind ourselves of what has happened so far on the audit. Having gained an understanding of the client, identified and assessed risk, formulated an audit plan, the auditor is in a position to carry out further audit procedures. These procedures are usually performed on ***samples*** of populations e.g. sales, debtors, creditors. Audit conclusions, however, must be drawn about the ***populations*** from which the samples came; therefore if there are errors in the sample, the auditor must do the following:

4.1 Analyse and project the errors in the sample over the population sampled

If a statistical basis has been used for selecting the sample, the appropriate statistical method for projecting the error in the sample over the population, will be used. Most often however, auditing firms use a proportional projection method, e.g.

$$\frac{\text{error value in sample}}{\text{total value of sample}} \times \text{total value of population}$$

to obtain an idea of the extent to which the population is misstated. Whatever method of projection is used, if the projected misstatement for the population is unacceptable, the auditor must:

4.2 Decide whether further tests should be carried out by the audit team, or whether the client should be asked to check the population in detail for further errors.

After this process has been completed, the auditor must:

4.3 Discuss all misstatements with management in an attempt to have them rectified.

If management refuses to correct misstatements, the auditor is left with what are termed, uncorrected misstatements (commonly referred to as unresolved audit differences), and it is at this point that final materiality comes into play. The auditor must now decide whether the uncorrected misstatements are immaterial, i.e. their presence will not influence the decision of a user, or whether they are material. If they are material, failure to correct them will result in financial statements which contain more misstatement than is acceptable, i.e. some aspects of the financial statements are not "presented fairly", and the auditor will have to modify the audit opinion. Making this decision is not just a matter of deciding that final materiality will be equal to planning materiality and that any errors over the planning materiality level will be material. There are a number of factors to be considered at the evaluation stage. These are discussed in 4.4 below. At this point you may be asking yourself why management might not want to correct all misstatement. Most often they will, but sometimes they will not. The reasons for this are that management may:

* ***disagree that there is a misstatement***
  e.g. the auditor believes that a lease should be capitalised as a finance lease, but the client does not believe that it qualifies as a finance lease in terms of IAS 17,
  e.g. the client genuinely believes that their estimation of inventory obsolescence is fair but the auditor thinks it is too low

* ***not regard the misstatement as material*** i.e. management don't believe that leaving the misstatement uncorrected will influence a user's decision

* ***have ulterior motives*** e.g. the directors wish to achieve particular ratios which are based on figures in the financial statements. If corrections which the auditor requests are made, the ratios which management wish to achieve, will not be reflected

* ***regard it as "too much hassle" to make the changes,*** e.g. the adjustment would mean changing the income statement, statement of financial position, consolidation, supporting schedules, etc

* ***be unconcerned about receiving a qualified audit opinion.***

4.4 Factors to be considered in evaluating uncorrected misstatements

At the planning stage, the auditor used his professional judgement to set a level of misstatement which could be present in the financial statements without influencing the decisions of users. If the audit goes as expected and the auditor has no reason to change this planning materiality level, it is logical that any uncorrected misstatement should be measured against this planning materiality amount to determine whether it is material for final materiality evaluation purposes. However, as we indicated earlier, evaluating uncorrected misstatements is not just a matter of comparing the misstatement to a quantified amount and disregarding those that are below the amount as being ***immaterial***. As ISA 450 says, "the circumstances related to some misstatements may cause the auditor to evaluate them as material, individually or when considered together with other misstatements, even if they are lower than materiality for the financial statements as a whole."

* ***factual misstatements, judgemental and projected misstatements***
  - a "factual misstatement" is a misstatement that the auditor (and therefore the client) can clearly identify and substantiate with supporting evidence, e.g. sales invoices which have been included in the wrong period. They are misstatements about which there is no doubt,

  - a "judgemental misstatement" is a difference arising from the judgements of management concerning accounting estimates that the auditor considers

unreasonable, or the selection and application of accounting policies that the auditor considers inappropriate.

- a projected misstatement is the auditor's best estimate of misstatements in populations, involving the projection of misstatements identified in audit samples over the entire population from which the sample was drawn.

The auditor makes this distinction as it will affect the attitude or stance which is adopted when dealing with the treatment of the uncorrected misstatements. If the error is a factual misstatement, the auditor may be more forceful in requesting that the error be corrected, and if the client refuses, the auditor is on strong ground if he decides to qualify the audit opinion. Where it is a judgemental or projected misstatement, the auditor will have to be less forceful, and open to further discussion and negotiation with regard to insisting on correction and qualifying the report, because of the error's subjective nature.

* ***offsetting uncorrected misstatements against each other*** – it is theoretically unsound to offset uncorrected misstatements against each other to reduce the "effect" of misstatements. In other words, a material misstatement which results in an overstatement of say, R100 000 in inventory should not be offset against an understatement of say, R120 000 in accounts receivable (or an overstatement of accounts payable) to reduce the "misstatements" to a net of R20 000. Likewise as indicated in ISA 450, if revenue has been materially overstated, the financial statements as a whole will be materially misstated, even if the effect of the misstatement on earnings has been completely offset by an equivalent overstatement of expenses.

* ***circumstances*** related to some misstatements may cause the auditor to evaluate them as material even if they are lower than materiality for the financial statements as a whole. Circumstances that may affect the evaluation include the extent to which the misstatement:
  - ***affects compliance with regulatory requirements***, e.g. the misstatement or omission of amounts relating to directors remuneration may be regarded as material even though the amounts are below the materiality level
  - ***affects compliance with debt covenants or other contractual requirements*****,** e.g. an uncorrected misstatement in inventory may not be material in terms of the materiality level but may affect compliance with a requirement (covenant) in a loan contract that inventory does not exceed a certain amount or percentage of current assets
  - ***impacts on ratios or trends*** which are "popular" with users of the financial statements in evaluating the entity's financial position, results of operations or cash flows e.g. earnings per share
  - ***has the effect of increasing management earnings,*** e.g. a company may pay its management a bonus based on net profit, before taxation. Therefore all misstatements which affect net profit before tax which remain uncorrected, will also affect management's bonuses. Even though there may be a reluctance on the part of management to correct such misstatements, the audit may "insist" upon the correction of such misstatements even though they are not quantitatively material. Bonuses paid to management should be as accurate as possible
  - ***relates to items involving particular parties,*** e.g. contracts entered into by the company in which a director has a financial interest, should be disclosed. If the company omits this disclosure the auditor cannot disregard this misstatement on the grounds that the value of the contract is below the materiality level
  - ***reflects a level of dishonesty by the directors,*** e.g. if the materiality level is R100 000 for the accounts receivable balance and the auditor discovers that an unauthorized loan of R75 000 to a director has been "hidden" in the accounts receivable balance, the auditor cannot regard this as an ***immaterial misstatement*** because it is below the materiality level of R100 000.

  The list of circumstances given above is not exhaustive. It is, however, sufficient enough to illustrate that when evaluating the effect of uncorrected misstatements on

the financial statements, both quantitative and qualitative factors must be considered by the auditor.

* ***misstatements should not be considered in isolation*** - although each individual misstatement is considered to evaluate its effect on the relevant classes of transactions, account balances or disclosures, misstatements must be aggregated (added together) for evaluation purposes. Remember that an individual misstatement in say, inventory may be below the materiality level but when added to other individual misstatements which are also below the materiality level, the aggregate misstatement may be above the materiality level. Similarly, if misstatements are being measured against say, a materiality level for total assets, then the aggregate (total) of uncorrected misstatements relating to account balances making up total assets, must be used for evaluation purposes.

4.5 Should final materiality equal planning materiality?

The answer is that the final materiality which the auditor uses to evaluate uncorrected misstatements should be equal to the planning materiality eventually used on the audit. This of course, may not be the auditor's initial planning materiality because, as we have seen, the initial planning materiality can change as the audit progresses. But if you think about it, the planning materiality which the auditor eventually uses is his best estimate of the amount of misstatement users will accept in the financial statements, so uncorrected misstatements must be evaluated against this amount.

CONCLUSION

There is no magic formula which tells the auditor what the planning and performance materiality levels should be or how uncorrected misstatement should be evaluated. It is a matter of judging the circumstances of each client separately. You will no doubt feel uneasy with this topic, but this is not surprising – understanding the concept is straight forward, its application less so. The entire question of "what is material" and "how should it be addressed" causes most practitioners some concern and it is only years of experience which build confidence and improve professional judgement.

THE AUDITOR'S RESPONSIBILIES RELATING TO FRAUD IN AN AUDIT OF FINANCIAL STATEMENTS

INTRODUCTION

As a result of the increase in fraud worldwide, and in particular the now notorious frauds at Enron, Parmalat and LeisureNet, to name just a few, a lot of attention has been focused on the accounting profession. Such questions as "where were the auditors?", why didn't the auditors pick up the fraud?, have been asked repeatedly. Whilst these questions may be very simplistic and naïve, the profession moved quickly to address the issue by, inter alia, substantially increasing reference to fraud in its auditing pronouncements. ISA 240 – The auditor's responsibilities relating to fraud in an audit of financial statements, deals with this topic in some depth.

AUDITOR'S OBJECTIVE

In terms of ISA 240 – The objectives of the auditor are to

* identify and assess the risk of material misstatement of the financial statements due to fraud

* obtain sufficient, appropriate audit evidence regarding the assessed risk of material misstatement through designing and implementing appropriate responses

* respond appropriately to fraud or suspected fraud identified during the audit.

TERMINOLOGY – DEFINITIONS (compiled from various sources in ISA 240)

1. ***Error.*** This term refers to an ***unintentional*** act which results in misstatement in the financial statements and may include:

* a mistake in gathering or processing data from which financial statements are prepared, e.g.
  - mathematical or clerical mistakes (e.g. incorrect depreciation calculations)
  - omission of a transaction (e.g. failure to record a sale)

* oversight or misinterpretation of facts (e.g. charging incorrect rates of interest as a result of failing to understand the terms of the loan agreement).

* misapplication of accounting policies (e.g. capitalising an operating lease through ignorance of the financial reporting standards).

2. ***Fraud.*** This term refers to an ***intentional*** act by one or more individuals among management, those charged with governance, employees or third parties involving the use of deception to obtain an unjust or illegal advantage.

3. ***Fraud risk factors.*** This term relates to events or conditions that indicate an incentive or pressure to commit fraud or provide an opportunity to commit fraud.

4. ***Management fraud.*** This term relates to fraud involving one or more members of management or those charged with governance.

5. ***Employee fraud.*** This term relates to fraud involving only employees ***not*** management or those charged with governance.

6. ***Fraudulent financial reporting.*** Fraudulent financial reporting involves intentional misstatements, including omissions, in financial statements to deceive financial statement users, e.g. the directors deliberately understate the liabilities and overstate the assets of their company to secure a loan from a bank, or they manipulate earnings either to reduce taxation or increase their own performance based remuneration. Fraudulent financial reporting which will normally be perpetrated by management or those charged with governance, may be accomplished by the following

* ***manipulation, falsification or alteration of the accounting records or supporting documentation underlying the financial records e.g.***
  - changing the balance on a debtors account to reflect a higher value
  - inflating the cost price of inventories
  - including fictitious sales.

* ***misrepresentation in, or intentional omission from the financial statements, of events, transactions or other significant information e.g.***
  - omitting a significant contingent liability from the notes
  - underproviding or failing to provide at all for known future losses
  - failing to reflect the sale of material assets.

* ***intentional misapplication of accounting principles to amounts, classification, manner of presentation or disclosure e.g.***
  - failing to capitalise finance leases
  - intentionally using an inappropriate policy for revenue recognition to inflate profits.

* ***management override (particularly where controls appear to be operating effectively)***
  - recording fictitious journal entries to manipulate operating results or other balances e.g. raising fictitious sales by journal entry
  - inappropriately adjusting assumptions or changing judgements used to estimate account balances e.g. understating asset impairments
  - omitting, advancing or delaying recognition of events and transactions at reporting date, e.g. recognising profits on a long-term contract prematurely
  - concealing or not disclosing facts which could affect the amounts recorded in the financial statements
  - engaging in complex transactions structured to misrepresent the financial performance or position of the company e.g. manipulating inter company balances (in a group) to "reallocate" profits earned by the related companies
  - altering records and terms relating to significant or unusual transactions.

7. ***Misappropriation of assets.*** This involves the theft of an entity's assets and may be perpetrated by employees or management. Where management is involved, it is harder for the auditor to detect as it is easy for management to conceal or disguise the misappropriation. Misappropriation would include

* ***embezzlement***
  - stealing cash sales
  - stealing receipts from debtors (and writing off the debtor as bad)

* ***theft of physical assets or intellectual property***
  - stealing inventory for personal use or sale
  - selling the company's trade secrets to a competitor

* ***causing the entity to pay for goods and services not received***
  - paying wages to fictitious (dummy) employees
  - making payments to a (fictitious) company set up by management for goods which are never received

* ***using the company's assets for personal use***
  - hiring out the company's equipment at week-ends and keeping the fees charged or using the entity's assets as collateral (security) for a personal loan.

The distinguishing feature between fraud and error is ***intention***. In a sense errors are made in "good faith" whilst fraud is in "bad faith", there is an intention to misrepresent and thereby cause prejudice to some party. Although the distinguishing feature is intention, it is not always easy for the auditor to determine the intention of the directors. This is particularly true where there is a high level of subjectivity involved in the financial statement item in which the suspected misrepresentation has taken place, e.g. an estimate, or where there are options e.g. a range of possible accounting policies which could be adopted and which produce different results. There is no definite or conclusive way of

determining intention, but obviously the auditors assessment of the integrity of management will be an important consideration.

RESPONSIBILITY OF MANAGEMENT AND THOSE CHARGED WITH GOVERNANCE

The responsibility for the ***prevention*** and ***detection*** of fraud and error lies both with those charged with governance and with management. This responsibility should be met by the implementation and continued operation and monitoring of the system of internal control. Management and those charged with governance need to set the proper tone and create and maintain a culture of honesty and ethics, in other words a strong control environment. Although the auditor may make recommendations about internal control, it is management who carry the responsibility for a sound system of internal control. Management are also responsible for making a conscious assessment of the risk that the financial statements may be materially misstated as a result of fraud.

RESPONSIBILITIES OF THE AUDITOR

So where does this leave the auditor? ISA 240 lays down what is required of the auditor in respect of fraud. The auditor should:

1. Maintain an attitude of ***professional scepticism.*** In the context of the auditor's responsibility to fraud, this means that the auditor should not be "led around by the nose" by the client and simply accept what he is told regardless of who tells him. The auditor should realise that in today's business environment, fraud is widespread and therefore the risk of occurrence is high. In a nutshell, today's auditor must not be naive and believe that the intentions of the client are always honest and honourable. Even if management has acted with integrity in the past, the auditor cannot assume that they will continue to do so. Circumstances change. For example, the client may have become, in the past year, a subsidiary of a holding company which demands high levels of performance. Your client's management may be tempted into adopting dubious business practices and manipulating financial reports in an attempt to meet performance targets and avoid losing their jobs.

2. Facilitate the ***discussion*** of a client's susceptibility to material misstatement due to fraud, ***amongst the audit team***. Each member of the team should be aware of the circumstances/factors which may indicate fraud and should be aware of "what to look out for".

3. ***Conduct risk assessment procedures and related activities***

* when obtaining an understanding of the entity and its environment (ISA 315 (Revised)), the auditor should enquire of management as to
  - its assessment of the risk that the financial statements will be materially misstated due to fraud
  - its processes for identifying and responding to the risks of fraud including details of any fraud already identified (or which management considers likely)
  - its processes for responding to alleged fraud: e.g. a supplier notifies management that one of the company's buyers is taking kickbacks from other suppliers, what action is taken
  - its communication with those charged with governance regarding the identification of, and response to, fraud
  - how management communicates its stance on ethical behaviour to employees

* the auditor should make enquiries of management, those charged with governance, internal audit and others in the organisation (e.g. in-house legal counsel, the ethics officer, human resource manager, operating personnel not directly involved in financial reporting) to determine whether they have knowledge of any actual, suspected or alleged fraud.

* the auditor should obtain an understanding of how those charged with governance, exercise their responsibility to oversee management's processes for identifying and responding to the risk of fraud by
  - attending meetings at which such matters are addressed
  - reading minutes of such meetings

- direct enquiry of those charged with governance

* the auditor should consider unusual or unexpected relationships when performing analytical procedures to obtain an understanding of the entity and its environment, e.g. unexpected fluctuations in the gross profit percentage ratio may indicate fraudulent misstatements of the figures used in calculating the ratio e.g. inclusion of fictitious sales, overstatement of closing inventory etc.

* the auditor should consider information from other related activities e.g. information obtained at an interim audit, whilst conducting preliminary engagement activities.

* the auditor should consider whether the information gained when obtaining an understanding of the entity and its environment, indicates that one or more ***fraud risk factors*** are present, see fraud risk factors below.

4. Identify and assess the risk of material misstatement due to fraud at ***financial statement level*** and at ***assertion (account balance/transaction/disclosure) level***.

5. Determine an overall (audit) response to address the risk of material misstatement due to fraud at financial statement level and assertion level.

RESPONSES TO THE RISK OF MATERIAL MISSTATEMENT DUE TO FRAUD

1. ***At financial statement level.***

The auditor should

* consider the assignment (and supervision) of appropriate staff
  - competent and technically skilled (experts if necessary)
  - experienced
  - strongly independent (won't be bullied by client)
  - able to adopt the correct degree of professional scepticism

* consider the accounting policies adopted by management
  - appropriate and properly applied or
  - indicative of fraudulent financial reporting, chosen to manipulate earnings or to fraudulently influence the perceptions of users.

* incorporate an element of unpredictability in determining nature, timing and extent of testing. Management generally have some idea of what the auditor will do. Changing the nature, timing and extent of tests may throw management off balance, and upset their attempts at concealment of fraud. There should also be an increase in the need to corroborate management's explanations/representations concerning material matters.

2. ***At assertion level.***

The auditor should

* consider the nature, timing and extent of testing necessary to reduce the risk of material misstatement due to fraud being present, to an acceptably low level.

* The tests and procedures which the auditor has available in compiling the audit plan to address the risk of fraud, are no different to those which are used to respond to the risk of unintentional material misstatement. The auditor must still decide on what tests to do (nature), when to do them (timing), and how much to do (extent). However, when addressing an appropriate response to fraud, the auditor needs to remember that
  - those who have perpetrated the fraud will attempt to conceal it, making it far more difficult for the auditor
  - the most reliable and relevant evidence must be sought. There can be severe consequences arising out of fraud and the auditor needs to be on firm ground before either deciding there is fraud, or whether there is no fraud.

* Generally speaking, the nature of testing is likely to become more inclusive, e.g. inquiry supported by inspection and analytical review to provide more corroborative evidence coupled with more extensive testing. The auditor may also decide that due to management override, the focus should be on substantive testing; or that external or auditor-generated evidence must be sought, as opposed to relying on the representations of management or other internally generated evidence. The auditor may also decide that the use of experts is necessary (e.g. identifying fake goods) or that CAATs be used to extensively interrogate databases, e.g. searching for anomalies such as duplicate ID numbers, or duplicate bank accounts in an employee masterfile, when the inclusion of fictitious employees is suspected. With regard to the timing of tests, the auditor may decide to change "normal" timing by introducing surprise visits, in an attempt to catch the client (management) off guard, e.g. arriving unannounced to count and reconcile till cash (in a cash retail business), count inventory or conduct a physical verification of employees.

3. Management override.

The auditor should design and perform audit procedures to respond to the risk of management override. To respond to this risk the auditor should:

* test the appropriateness of ***journal entries and other adjustments*** made in the preparation of the financial statements (remember that even a system which produces valid, accurate and complete data, can be overriden by the passing of a journal entry to manipulate the balances or totals produced by that system). In deciding on which entries and other adjustments to select for testing, the auditor should consider

  - the presence of any ***fraud risk factors*** which might indicate journal entries related to fraud, e.g. there is an assessed risk that proceeds from debtors are being stolen and concealed by writing off the debtor as bad

  - the effectiveness of the client's ***controls over the authorization and implementation*** of all journal entries, and concentrate on those which are inadequately authorized or where implementation has been abnormal in terms of the internal control system

  - whether the ***characteristics of fraudulent journal entries*** and other adjustments are present. Such journal entries and other adjustments often reflect the following characteristics
    (i) entries are made to unrelated, unusual or seldom used accounts
    (ii) they are passed by individuals who do not normally make journal entries
    (iii) they are not supported by adequate reasons, explanations or descriptions
    (iv) they are not posted to specific ledger accounts, but rather directly to amounts in the financial statements at period end
    (v) contain round amounts or consistent ending numbers

  - the ***nature and complexity of the accounts*** used in the entry, e.g. fraudulent journal entries may be made to accounts which contain transactions which are complex or unusual, are not reconciled regularly, or which seem to have no specific purpose, such as "slush funds"

  - whether the journal entry is outside of the ***normal course of business***, i.e. non-recurring. Because non-recurring journal entries are not normally addressed by the internal control system, there is a greater chance that they will be fraudulent

* review accounting estimates for biases which could result in material misstatement due to fraud, e.g. deliberate understatement of allowances such as obsolete inventory, bad debts, depreciation/impairment, to intentionally manipulate earnings figures.

* obtain an understanding of the business reasons of significant transactions outside of the normal course of the company's business, or that otherwise appear to be unusual e.g. the company suddenly purchases another company which manufactures a completely different and unrelated product to that which the company itself manufactures.

4. Evaluation of evidence.

The auditor should consider whether the assessment of material misstatement at assertion level remains appropriate once the initial planned audit procedures have been conducted (ISA 330). In actually carrying out the planned audit procedures, the auditor may be alerted to the possibility of fraud by the existence of numerous situations or circumstances. ISA 240 provides a lengthy list of these circumstances which individually or in combination, indicate the possibility that the financial statements may contain material misstatement resulting from fraud. Some examples have been listed below to illustrate.

Discrepancies in the accounting records

* bank and other reconciliations are not conducted timeously
* unauthorised transactions e.g. unathorised travel expenditure
* evidence of employees' access to systems and records inconsistent with that necessary to perform their authorised duties, e.g. a factory foreman has access to the employee masterfile
* tips or complaints to the auditor about alleged fraud, e.g. fraud hotlines
* last minute adjustments that significantly affect financial results.

Conflicting or missing evidence

* missing documents or documents which appear to have been altered e.g. purchase transactions selected for testing are not supported by purchase orders or supplier delivery notes
* unexplained items on reconciliations
* unexplained changes in trends, ratios or relationships, e.g. increase in sales commission expense but no increase in sales
* inconsistent, vague or implausible responses from management or employees arising from inquiries or analytical procedures
* payments for services (e.g. to lawyers, consultants or agents) that appear excessive in relation to the services provided
* unusual discrepancies between the entity's records and external confirmation replies
* missing inventory or physical assets, revealed by existence testing
* unavailable or missing electronic evidence inconsistent with the company's retention practices.

Problematic or unusual relationships between the auditor and management

* denial of access to records, facilities, certain employees, customers etc.
* undue time pressures imposed by management to resolve complex or contentious issues, or unrealistic audit deadlines
* management intimidation (or attempted intimidation) of engagement team members
* unusual delays by the entity in providing requested information
* unwillingness to agree to the use of (reasonable) CAATs (particularly where there is no realistic alternative method of gathering evidence)
* an unwillingness to address identified weaknesses in internal control on a timely basis
* general lack of co-operation.

Other

* unwillingness by management to permit the auditor to meet privately with those charged with governance
* changes in accounting estimates that do not appear to result from changed circumstances
* tolerance of violations of the entity's code of conduct.

Note: The auditor will also consider whether an identified misstatement (not initially thought to be fraud) is in fact fraud. In effect this will be an assessment of whether the misstatement is intentional. If so, the auditor should consider the effect of this (fraud) on the rest of the audit, especially other representations made by management.

5. Management representations.

The auditor should obtain written representations from management relating to fraud. These representations should

* contain management's acknowledgement that it is responsible for the design, maintenance and implementation of internal control to prevent and detect fraud
* state that management has disclosed to the auditor, the results of its assessment of the risk that the financial statements may be materially misstated as a result of fraud

* state that management has disclosed to the auditor, its knowledge of fraud or suspected fraud involving
  - management
  - employees
* state that management has disclosed to the auditor any allegations of fraud or any suspected fraud affecting the entity's financial statements communicated by employees, former employees, analysts, regulators or others.

FRAUD RISK FACTORS

1. Introduction

When gaining an understanding of the entity and its environment and assessing the risk of material misstatement due to fraud, the auditor must consider whether the information obtained, indicates the presence of fraud risk factors. ISA 240 divides these factors into two categories, namely

* ***risk factors relating to misstatement resulting from fraudulent financial reporting.*** These are factors which indicate to the auditor that the financial statements may be manipulated to achieve fraudulent financial reporting

* ***risk factors relating to misstatements resulting from misappropriation of assets***.

The statement then suggests that each of the above categories should be looked at from the perspective of

* ***incentives/pressures,*** i.e. are there incentives for, or pressures on management to report fraudulently or for management or employees to misappropriate assets?

* ***opportunities***, i.e. are there opportunities for fraudulent financial reporting or misappropriation of assets?

* ***attitudes/rationalizations***, i.e. does the attitude and behavioural manner of management and employees, suggest an environment conducive to fraudulent reporting or misappropriation of assets?

The following examples are presented to illustrate the above. A more comprehensive list can be found in ISA 240. Bear in mind that where fraud is being perpetrated, a number of risk factors are likely to be present.

2. Fraudulent financial reporting

2.1 Incentives/Pressures

These factors may provide incentive or place pressure on management to engage in fraudulent financial reporting or the factors may indicate that management have reported fraudulently.

* ***Financial stability or profitability is threatened by economic, industry or entity operating conditions***
  - high degree of competition accompanied by declining margins
  - high vulnerability to rapid changes, such as changes in technology, product obsolescence, or interest rates, e.g. electronics companies
  - operating losses threatening going concern
  - new accounting, statutory, or regulatory requirements (e.g. the application of new environmental legislation relating to certain chemical products will significantly affect the saleability of the company's inventory)

* ***Excessive pressure exists for management to meet the requirements or expectations of third parties due to the following:***
  - profitability or trend level expectations of investment analysts, institutional investors, significant creditors, or other external parties.
  - the need to obtain additional debt or equity financing to stay competitive, e.g. manipulating financial statements used to support a loan application.

- difficulty in meeting debt repayment or other debt covenant requirements, e.g. manipulating the financial statements to maintain prescribed financial ratios specified in a loan agreement.
- perceived or real adverse effects of reporting poor financial results on significant pending transactions, such as a merger or the awarding of a contract, e.g. a construction company reporting financial losses, having recently tendered for a large contract to construct an office block.

* ***Information which indicates that the personal financial situation of management is threatened by the entity's financial performance arising from the following:***

- significant personal financial interests in the entity, e.g. management hold significant numbers of shares
- significant portions of their compensation (e.g. bonuses, share options are contingent upon achieving aggressive targets for operating results, financial position or cash flow, e.g. the gross amount of management bonuses is 25% of net profit after tax
- personal guarantees of debts of the entity, e.g. directors have given personal guarantees for the debts of the company.

* ***There is excessive pressure on management to meet financial targets established by those charged with governance, including sales or profitability incentive goals.***

2.2 Opportunities

These factors are examples of conditions/situations which provide the opportunity for management to engage in fraudulent financial reporting.

* ***The nature of the industry or the entity's operations***

- significant related-party transactions particularly where the related party is not audited by the same firm.
- a strong financial presence or ability to dominate a certain industry sector that allows the entity to dictate terms or conditions to suppliers or customers that may result in inappropriate or non-arm's length transactions.
- assets, liabilities, revenues, or expenses based on significant estimates that involve subjective judgements or uncertainties that are difficult to corroborate, which can be used to manipulate results.
- significant, unusual, or highly complex transactions, which can be used to manipulate results.
- use of business structures or business methods for which there appears to be no clear business justification, e.g. importing goods indirectly through a neighbouring country.

* ***Ineffective monitoring of management***

- domination of management by a single person or small group (in a non owner-managed business) without compensating controls.
- ineffective oversight by those charged with governance over the financial reporting process and internal control.

* ***A complex or unstable organisational structure, as evidenced by the following:***

- difficulty in determining the organisations or individuals that have a controlling interest in the entity.
- overly complex organisational structure involving unusual legal entities or unusual managerial lines of authority.
- high turnover rates of senior management, legal counsel, or those charged with governance.

* ***Internal control components that are deficient as a result of the following:***

- inadequate monitoring of controls.
- high turnover rates or employment of ineffective staff in accounting, internal audit, or information technology.
- ineffective accounting and information systems.

2.3 Attitudes/Rationalisations

These are factors or situations which may indicate that management may be predisposed to fraudulent financial reporting:

* ineffective enforcement of the entity's values or ethical standards by management, or the presence of inappropriate values or ethical standards

* non-financial management's excessive participation in selecting accounting policies or the determination of significant estimates. (This suggests they have a personal financial interest in reported earnings)

* history of allegations against members of management etc, for fraud or violations of laws and regulations (e.g. insider trading)

* excessive interest by management in maintaining or increasing the entity's share price or earnings trend

* an interest by management in employing inappropriate means to minimise reported earnings for tax-motivated reasons, e.g understating sales

* the owner-manager makes no distinction between personal and business transactions, e.g. takes holidays and charges the cost to the company

* the relationship between management and the auditor is strained, e.g. domineering or dismissive management attitude towards the audit team.

3. Fraud risk factors relating to misstatements resulting from misappropriation of assets

The presence of the following conditions or factors should alert the auditor to the possibility of misstatement arising from misappropriation of assets:

3.1 Incentives/Pressures

These factors provide incentive for management or employees to misappropriate assets

* personal financial problems.

* adverse relationships, between the entity and its employees including management, e.g. dissatisfaction with compensation or other conditions of service, or anticipated retrenchments (employee lay offs).

3.2 Opportunities

These fraud risk factors pertain to the ***nature*** of an entity's assets, the degree to which they are subject to theft, and the lack of ***internal control*** related thereto.

Nature

- large amounts of cash on hand.
- inventory characteristics, such as small size combined with high value and high demand e.g. jewellery, ipods.
- easily convertible assets, e.g. bearer bonds or diamonds.
- fixed asset characteristics, such as small size, marketability and lacking in ownership identification, e.g. hand-held power tools.

Internal control

- inadequate segregation of duties, e.g. storeman has "write access" to inventory records.
- lack of appropriate management supervision e.g. no supervision and observation of goods being taken into or despatched from the warehouse.
- lack of procedures to screen job applicants for positions where employees have access to assets susceptible to misappropriation (poor personnel practices).
- inadequate record keeping for, and reconciliation of assets (theoretical to actual)
- lack of an appropriate system of authorisation and approval of transactions e.g. acquisition of, and payment for, purchases.
- poor physical safeguards over cash, investments, inventory or fixed assets.

- lack of timely and appropriate documentation for transactions e.g. allowing customers to take goods, but doing the paper work later.
- lack of mandatory vacations for employees performing key control functions. Employees who are involved in fraudulent activities usually do not want to take a holiday as being absent makes it very difficult for that person to cover their tracks or conceal their fraudulent activities.
- inadequate authorisation and review of senior management expenditures e.g. travel claims.
- inadequate management understanding of IT which enables IT employees to do "what they like".

3.3 Attitudes/Rationalisations

These are factors which indicate that management/employees have a relaxed, casual or negative attitude towards controls relating to the prevention of misappropriation of assets.

* poor control environment e.g. ignoring incidents of theft, and overriding controls

* changes in behaviour or lifestyle that may indicate assets have been misappropriated e.g. management taking expensive holidays, driving expensive cars etc

* behaviour on the part of the employees (including management) which indicates displeasure or dissatisfaction with the entity or its treatment of its employees.

COMMUNICATION WITH MANAGEMENT, THOSE CHARGED WITH GOVERNANCE AND OTHERS

1. Introduction

If the auditor identifies misstatement resulting from fraud, appropriate action will need to be taken. Before proceeding there are a number of matters to which the auditor will need to give consideration, to ensure that his actions are appropriate.

* ***confidentiality*** – the auditor is bound by confidentiality and cannot simply inform all and sundry about the fraud e.g. it would be inappropriate to make direct contact with SARS, a creditor, a trade union.

* ***management involvement in fraud*** – fraud is by no means perpetrated only by (non-management) employees. The majority of large financial frauds are perpetrated by management, often including the directors. If the auditor believes that management is involved, great care must be taken in deciding to whom the fraud should be reported.

  In principle fraud should be reported to the level of authority above the level at which it has been perpetrated or is suspected. For example, if a wage fraud is perpetrated by the paymaster, it should be reported to the financial accountant. If the financial accountant is also suspected of being involved, it should be reported to the financial director. If the financial director is also suspected of being involved, it should be reported to the Chairperson of the Board or the audit committee (those charged with governance). And of course if none of this proves successful, it may be necessary to report the matter to the IRBA as a "reportable irregularity."

* ***absolute evidence of fraud?-*** whilst the auditor does not have to have absolute proof of fraud before taking action, he should make certain that he has obtained sufficient, appropriate evidence to support his contention and should be careful not to make direct accusations. The entire matter should be documented.
  Note also that for a "reportable irregularity" (which many frauds will be) to become "reportable" in terms of the Auditing Profession Act Sec 45, the auditor needs only to "have reason to believe" that the reportable irregularity is taking place, not absolute evidence.

2. Parties with whom the auditor might communicate concerning fraud

There are a number of individuals/parties with whom the auditor may communicate

* ***management (other than the Board of Directors)*** – as indicated earlier, the general principle is that fraud should be reported to the level above the level at which the fraud has been perpetrated. The auditor will need to decide
  - whether the "level above" is sufficiently high in the organisation e.g. a major fraud

conducted by a wage clerk would probably be reported to the financial director not only the paymaster
- whether the "level above" is in any way involved in the fraud, in which case it should be reported to a higher level.

* ***those charged with governance of the company*** – whilst management other than the Board, are responsible for the day to day implementation and application of practices and procedures which uphold proper governance, the Board of Directors is ultimately responsible for good governance. In addition, the Companies Act 2008 requires that public companies appoint audit committees. Audit committees share the responsibility for good governance. The decision the auditor will need to make is whether it is necessary to report the fraud to the Board and the audit committee. In general terms the auditor should report the following:
- material weaknesses in internal control (this means management are not meeting their responsibility and risk of fraud is increased)
- issues regarding management integrity
- fraud involving management
- other fraud that results in material misstatement of the financial statements

* ***regulatory and enforcement authorities -*** once again the auditor's duty of confidentiality would preclude reporting fraud to a 3rd party. However, the duty of confidentiality is overridden in certain circumstances where
- a reportable irregularity is reported to the IRBA in terms of Sec 45 of the AP Act
- the court or statute requires that such information be disclosed
- the client gives permission

* ***a proposed successor auditor -*** the question arises as to whether an auditor who has resigned (or is about to be replaced) may disclose details of fraud or suspected fraud to the proposed (successor) auditor. The Code of Professional Conduct requires that the proposed auditor should communicate with the existing auditor to establish whether it would be appropriate for the proposed auditor to accept the engagement. The extent to which the existing auditor may discuss the affairs of the client will depend on whether the client has given the existing auditor permission to discuss the affairs of the client with the proposed auditor. If permission has ***not*** been granted, the existing auditor may ***not*** discuss the affairs of the client with the proposed auditor, but should convey to the proposed auditor that permission has been refused.

FRAUD AND RETENTION OF CLIENTS

1. Should an auditor continue to service a client company at which fraud is a frequent occurrence? The answer is that where there is a high incidence of fraud, there is high audit risk and ultimately it is not in the best interests of an individual firm, or the profession as a whole, to retain such a client, particularly if management or those charged with governance will not take decisive action to eradicate fraudulent practices.

2. An auditor who resigns on the grounds that there is too much fraud or suspected fraud at a client company, will have to consider very carefully whether or not the fraudulent activities at the client constitute a reportable irregularity. If so, the auditor must fulfil his obligations in terms of Sec 45 of the Auditing Profession Act ***before*** resignation.

3. The auditor should also consider his overriding duty to act in a professional manner, with honesty and integrity and to fulfil his duty to conclude the audit. The auditor should make every attempt to fulfil his reporting obligations – that is precisely why he has been appointed. To resign from an engagement, especially before the expiry of his term of office, should not be an easy option taken simply to avoid getting into a time consuming, confrontational or otherwise unpleasant situation, and doing so may have legal consequences for the audit firm.

CONSIDERATION OF LAWS AND REGULATIONS IN AN AUDIT OF FINANCIAL STATEMENTS - ISA 250

1. INTRODUCTION

This statement gives guidance on the auditor's responsibilities with regard to the non-compliance by the client with the laws and regulations which govern the client's business.

2. IMPORTANT CONSIDERATIONS

* There are often numerous laws and regulations which govern the client's business, e.g. environmental, operating, income tax and health legislation to mention but a few, as well as municipal, regional council and industry regulations.

* The auditor is not expected to have an in-depth knowledge of all these laws and regulations but should be aware of those which, ***if not complied with,*** could have a material effect on the financial statements. Some of these are easy to identify : all auditors should be aware of the consequences of non-compliance with the Companies Act or the Income Tax Act and very often the effect on the financial statements is reasonably quantifiable. However, non-compliance with other laws and regulations may not be quite so obvious to the auditor (but see para 3 below). For example, non-compliance with the Road Transportation Act may result in heavy fines or the suspension of a licence. The latter penalty could seriously affect the going concern ability of the entity.

* The average auditor is not an expert in legal matters and may therefore not be able to determine whether there has been non-compliance by the client. This does not let the auditor off the hook; the procedures indicated below should be carried out and if, as is likely, legal opinion is required, the auditor should seek it.

3. AUDITOR'S DUTIES, RESPONSIBILITIES AND PROCEDURES

* The auditor has no responsibility to prevent non-compliance, that responsibility rests with management and those charged with governance.

* When complying with ISA 315 (Revised) – Identifying and assessing the risk of material misstatement, the auditor should consider the risk of material misstatement being present in the financial statements arising from the client's noncompliance with laws and regulations. The general principle of professional scepticism should prevail throughout the audit.

* When gaining an understanding of the entity and its environment, the auditor should obtain a general understanding of the laws and regulations which govern the client. The auditor will commence by identifying such laws and regulations, e.g. if the company is listed and involved in foreign transactions (very likely) and road transportation, the audit team should be appraised of the salient features of the JSE regulations and the acts which govern foreign exchange transactions and road transportation, and instructed to be alert to the possibility of non-compliance with these laws and regulations. This would extend to the performance of tests ***specifically*** to identify noncompliance, e.g. enquiries may be made of management and third parties, and documents may be inspected to confirm that the client is complying with any regulation or law which is critical to its continued existence and which has a bearing on fair presentation if there has been non-compliance.

* During the performance of the audit, the auditor must be alert to evidence which could indicate that non-compliance has occurred. Some examples are as follows:
  - investigation of the client's affairs by government or regulatory bodies
  - the payment of fines or penalties
  - material transactions for which there is inadequate or insufficient supporting documentation e.g. unsupported payments to government employees, related parties,
  - unusual transactions, e.g. what is the reasoning? Is there an attempt to get around the law?
  - large cash payments, e.g. paying bribes? laundering money? buying stolen goods?
  - purchase at non-market prices, e.g. why would the company pay more than the market price?
  - excessive salesperson or agents commissions, e.g. why are the commissions higher than

the market?

- newspaper articles or news reports which suggest the occurrence of illegal practices in the particular industry in which the client operates, e.g. the importation of false brandname goods.

As mentioned earlier the auditor should view the presence of any of the above with professional scepticism.

* If the auditor becomes aware of a possible instance of noncompliance, the auditor should gather sufficient evidence to evaluate:
  - the potential financial consequences, such as fines, damages, litigation, expropriation of assets
  - whether adjustment to, or disclosure in, the financial statements, is required
  - whether failure to adjust or disclose, the financial consequences of non-compliance will result in a failure on the part of management, to achieve fair presentation of the financial statements.

* All findings should be documented and discussed with management.

4. REPORTING OF NON-COMPLIANCE

As with the reporting of fraud, the auditor may need to report to various bodies; the principles are the same as for reporting fraud.

1.1 To management and those charged with governance

The auditor should report as soon as practicable, to the audit committee, the board of directors and to senior management. The principle of reporting to a higher level than the level perpetrating the non-compliance, still holds. If the auditor believes that management is intentionally failing to comply with laws and regulations, it will be necessary to consider whether the non-compliance constitutes a reportable material irregularity in terms of the Auditing Profession Act 2005 Sec 45.

4.2 To users of the financial statements

If the auditor concludes that non-compliance which has a material effect on the financial statements, has not been adequately dealt with in the financial statements, the audit report should be modified accordingly. The audit report is the appropriate medium to report to users, and to communicate in other ways, without client consent, would be a breach of confidentiality.

4.3 Regulatory and enforcement agencies

Normally the auditor's duty of confidentiality would preclude him from reporting to third parties. However, in terms of certain statute, e.g. the Auditing Profession Act, or regulatory requirements, this duty may be overridden. If in doubt, the auditor should seek legal council before communicating any information pertaining to the non-compliance by the client.

CHAPTER 8

COMPUTER AUDIT
THE BASICS

CONTENTS

			Page
COMPUTER AUDITING			
1.	Introduction		8/3
2.	The components of internal control and information technology systems		8/4
	2.1	Control environment	8/5
	2.2	The company's risk assessment procedures	8/5
	2.3	The information system including business processes	8/5
	2.4	Control activities	8/6
	2.5	Monitoring of controls	8/6
GENERAL CONTROLS			
1.	Definition of a general control		8/7
2.	Categories of general controls		8/7
3.	Control environment		8/8
4.	Systems development and implementation controls		8/11
5.	Access controls		8/16
6.	Continuity of operations		8/22
7.	System software and operating controls		8/24
8.	Documentation		8/25
APPLICATION CONTROLS			
1.	Description		8/26
2.	Understanding control activities in a computerised accounting system		8/27
	2.1	Introduction	8/27
	2.2	Segregation of duties	8/27
	2.3	Isolation of responsibilities	8/28
	2.4	Approval and authorisation	8/28
	2.5	Custody	8/29
	2.6	Access controls	8/30
	2.7	Comparison and reconciliation	8/31
	2.8	Performance reviews	8/32
3.	Control techniques and application controls		8/32
	3.1	Batching	8/32
	3.2	Screen aids and related features	8/34

3.3 Programme controls - Input and processing 8/35
3.4 Output controls 8/38
3.5 Logs and reports 8/39

4. Masterfile amendments (masterfile maintenance) 8/39

COMPUTER ASSISTED AUDIT TECHNIQUES (CAATs)

1. Introduction 8/41

2. How do CAATs fit into the audit process? 8/41

3. System orientated CAATs 8/43

4. Data–orientated CAATs 8/45

5. Factors which will influence the decision to use CAATs 8/45

6. Audit functions which can be performed using data orientated CAATs and Appendix 1 8/46

THE USE OF MOBILE INFORMATION AND COMMUNICATION TECHNOLOGY ON AUDITS

1. What this technology can do 8/48

2. Security implications of using mobile information and communications technology on audits 8/49

COMPUTER AUDITING

1. INTRODUCTION

As an auditor, whether internal or external, junior or senior, you will be exposed to computerised financial reporting systems at your audit clients. You will also make use of laptop computers to assist you in carrying out your audit work. The vast majority of businesses you will visit to perform audits will make use of computers to capture, process and record transactions, produce the accounting records and lots of other information. However, the extent to which business entities use computers will vary considerably. A small company may have one or two stand alone personal computers onto which simple bookkeeping programmes are loaded. A large company will have a far more complex arrangement, using micro-computers as servers and workstations. Such companies will have data centres and lots of highly qualified personnel. You can deduce from this, that the range of skills required by auditors will be very diverse. The following two chapters are intended to provide you with a basic knowledge of computers in the context of auditing. As with most aspects of auditing, you are not expected to be an expert when you start going out on audit, but a basic knowledge of "computers" will help and is expected. For example, even very small businesses these days pay salaries and creditors by electronic funds transfer, so some knowledge of how this is controlled will be important if you are auditing the payroll or acquisitions and payments cycles. An understanding of general controls, application controls, masterfile amendments, etc, will give you a solid starting point. If you become a computer audit specialist, lots of additional study and experience will be needed!

You also need to get used to the fact that every business has different information needs. Different programmes do a multitude of different things and will be supported by different policies and procedures. Documents (both on screen and hardcopy) will be designed to meet users' specific needs and terminology will vary considerably. When you start work the detail will become second nature to you, but for study purposes you need to concentrate on the basics.

In this text we have used the term "computer environment" to describe any particular and unique combination of hardware, software and personnel. As briefly explained above, a small business is going to have a very different computer environment to a large company, and medium size companies are going to fit somewhere in between.

In the early days of business computing, had you gone to a large company's computer department, you would have been confronted by the central processing unit (a great big "box") with large storage devices (tape drives and disk drives) as well as terminals and printers. There would also have been IT personnel going about their business, e.g. capturing data, loading tape drives, monitoring what the computer was doing, loading the printers with specific stationery necessary for a particular job. Systems analysts, programmers, operators, technical personnel would also have been about. Generally the computer centre would have been a busy, but orderly place. However, with the development of the silicon chip, came the microcomputer which allowed CPUs and other devices to decrease substantially in size. Microcomputers have their own CPU and storage capabilities and this has enabled many businesses to replace mainframe and minicomputers with microcomputers. The age of end user computing was born. The result of this was that many of the functions which were performed in the computer centre are now carried out by users sitting at their workstations often with a printer nearby. The user is now responsible for entering data, carrying out checks, printing documents, etc, so the centralisation of computing facilities and operations has diminished dramatically. However, large companies still have vast amounts of highly technical equipment on which the computer systems are run and into which users are connected. This equipment, e.g. lots of servers doing different things, routers, modems, etc is still usually centrally located, (but does not have to be), in a physically protected area called the "data centre". The data centre will itself, not be inhabited by lots of employees.

The important point about all this from an auditor's perspective is that a client's computer environment will directly affect the audit strategy and plan. To illustrate:

* the strategy adopted to audit a bank will definitely call for the inclusion of computer audit experts on the team due to the complexity and importance of the computerised systems. The

fact that banks process millions of transactions will require that the strategy focus on tests of controls which in turn will affect the audit plan

* the strategy for the audit of a small company with a bookkeeper or two and a number of PCs will not require specialist computer skills and will probably be focused on substantive testing
* the software used by a large company is likely to be far more sophisticated, highly integrated (simplistically this means that applications work together, e.g. a credit sale automatically updates the inventory records, and the debtor ledger and general ledger), and have many more control features for input, processing and output. At the other end of the scale, a small business may use simple software for each application which is not linked to any other application, e.g. a simple computerised perpetual inventory application may require that all movements of inventory e.g. receipts, issues of inventory items will be entered onto the system by keying in the information from hardcopy goods received notes (GRNs) and delivery notes. The difference in the capabilities of the software will directly affect the validity, accuracy and completeness of the information it produces as well as the way in which the information is audited
* as a final illustrative example, the use of audit software (i.e. software which helps the auditor conduct the audit or carry out what are termed "computer assisted audit techniques") will be absolutely critical on some audits, and hardly critical at all on others. For example, the efficient and effective audit of debtors for a large company with say, 5 000 debtors, will not be possible without using audit software to interrogate the debtors masterfile, extract samples from it, reperform calculations, analyze it, etc. In a small business with say, 200 debtors, this may not be necessary or even possible. In this situation it may be far more efficient to carry out manual audit procedures.

Bear in mind that generally the more sophisticated the software is, the more it costs to purchase and run. These days software has more features than any business could desire, but many of the features do not provide any great benefit, so companies use cheaper software and/or "enable" only those controls and features the business needs. In principle, this is no different from how you use your cell phone, ipad, or laptop!

Regardless of whether the company is small, medium or large, hardly computerised or extensively computerised, management is still responsible for implementing and maintaining control, and the auditor still goes through the audit process as described and discussed in chapter 6 and 7.

One of the specific objectives of internal control is to achieve reliable reporting; in computer "speak" this is often referred to as the production of information by the information system (of which the accounting system is part) which is valid, accurate and complete. From the auditor's perspective, if the information produced, is valid, accurate and complete the risk of material misstatement in the financial statements is significantly reduced.

Finally, computer environments are sometimes distinguished as ***personal usage, small business systems*** and ***large business systems***. This is a useful way of classifying them and reminding us that different audit strategies and plans are required for different businesses.

2. THE COMPONENTS OF INTERNAL CONTROL AND INFORMATION TECHNOLOGY SYSTEMS

Internal controls can be defined as the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to:

* the reliability of the entity's financial reporting
* the effectiveness and efficiency of its operations and
* its compliance with applicable laws and regulations.

One of the best ways by which management can achieve these objectives is by embracing the ever increasing power and versatility of information technology. For example, a company computerizes its accounting system to improve the reliability of its financial reporting system because computers can process vast quantities of

information very accurately and very quickly, can store information for instant retrieval, can analyse information extensively and communicate it instantly and widely.

In terms of ISA 315 (Revised), the auditor is required to gain an understanding of the company's internal control system and the statement suggests that this understanding can best be obtained by considering the 5 components of internal control. These components are:

* the control environment
* the company's risk assessment procedures
* the information system, including related business processes relevant to financial reporting
* control activities
* monitoring of controls

It stands to reason therefore, that when considering each component the auditor will need to consider the effect of the company's IT (computerization) on that component. For example, when evaluating the company's control environment the auditor will look specifically at the control environment relating to IT management.

2.1 Control environment

This is about management's attitude to and awareness of the need for controls. Because of the potential major consequences of poor control in a computerised system, a strong control environment is very important. The evaluation of the control environment will be far more intense in a large, highly computerised company (think bank!) than in a smaller or medium size business. Evaluation of the control environment is discussed extensively in chapter 5 and later in this chapter.

2.2 The company's risk assessment procedures

In the context of a computerised environment this component is about controlling IT risk. The King III report on corporate governance recognizes information technology (IT) risk as one of the major risks facing a company (particularly a large company). Whilst managing IT risk is the responsibility of the board, it is likely that the board will delegate its responsibility to a risk committee. The structures of the IT section may include a steering committee and a chief information officer. Part of this internal control component's function will be to focus on the assessment of (and response to) the IT risks facing the company e.g. data security and privacy, business continuity, data recovery and keeping up with technology etc.

2.3 The information system, including business processes relevant to financial reporting

The information system consists of infrastructure (physical and hardware components) software, people, procedures and data. When the auditor is gathering information about this component he will need to familiarize himself with each of the above and how they interact (refer to chapter 7 pages 7/15 to 7/17). ISA 315 (Revised) explains that the information system relevant to financial reporting objectives, which includes the accounting system, consists of the procedures and records designed and established to

* initiate, record, process and report entity transactions, events and conditions and to maintain accountability for the related assets, liabilities and equity
* resolve incorrect processing of transactions
* process and account for system overrides, e.g. by the creation of audit trail in the form of a log of overrides
* transfer information from transaction processing systems to the general ledger e.g. where the revenue application software is not integrated with the general ledger, a journal entry will have to be passed to get sales and debtors totals into the general ledger
* capture information other than transactions, such as depreciation and allowances for bad debts
* ensure information required for disclosure is accumulated, recorded, processed, summarized and appropriately reported in the financial statements
* authorize and process journal entries.

This knowledge provides the auditor with a basis to evaluate both the manual and automated procedures and controls which make up the next component of internal controls i.e. control activities.

2.4 Control activities

This is the component of internal control which will probably interest the auditor the most because these control activities (policies and procedures) have a big influence on whether the financial information system records and processes only transactions which are authorised and have already actually occurred, and does so accurately and completely.

It is important to remember that control activities in a computerised system will be a combination of manual and automated (programmed) controls. Modern software is packed with features which improve control over input, processing and output of data and it will be the auditor's duty to establish what features (automated controls) are in use at the client.

2.5 Monitoring of controls

This is the fifth component of internal control as identified by ISA 315 (Revised) and concerns management's responsibility to assess whether the internal control system is meeting its objectives over time. It is not solely about monitoring whether the control activities are taking place, it is also about assessing whether they are affective. Monitoring is also not only about assessing control activities, it is also about evaluating the other components of the internal control system, e.g. the control environment and the risk assessment process. In a computerised environment the amount and variety of information which can be quickly and accurately obtained from the system enhances the ability of management, those charged with governance as well as various bodies such as the internal audit department, audit and risk committees, to conduct effective monitoring over time.

GENERAL CONTROLS

1. DEFINITION OF A GENERAL CONTROL

Controls in a computerised environment are categorised as either ***general controls*** or ***application controls.*** General controls are those which establish an overall framework of control for computer activities. They are controls which should be in place before any processing of transactions gets underway and they span across all applications. In contrast, application controls are controls which are relevant to a specific task within a cycle of the accounting system, e.g. taking an order from a customer, filling the order, and preparing the invoice. For example, control procedures and policies to ensure that staff are competent and trustworthy, would be regarded as ***general*** controls, whilst a control procedure which requires that the foreman authorise all overtime worked, would be an ***application*** control (payroll cycle).

2. CATEGORIES OF GENERAL CONTROLS

Even a quick reference to the relevant literature reveals there are numerous ways of categorizing or classifying general controls. Whilst this can be confusing, it is not that important. What is more important is that you understand both the distinction between a general control and an application control and the kinds of general control you are likely to encounter at a client.

The auditor is required to obtain an understanding of the entity and its environment, and this will include obtaining an understanding of the general controls at the client. It is important to realize that the amount of knowledge and skill as well as the nature, timing and extent of procedures to obtain the necessary understanding will vary considerably from client to client. For example, the general controls at a small company which has a limited number of computers, does not employ its own specialized IT personnel, makes use of packaged application software, and uses an external computer consultancy to "keep its system up and running", will be very different to the general controls at a large company, particularly a company, such as a bank, which is highly dependent on computerised systems. During your period of training as an auditor it is unlikely that you will be given the responsibility for evaluating general controls at anything other than a small company because specialist knowledge is required. You may, of course, be required to assist in an evaluation of general controls for a larger company. Either way, a basic knowledge of what general controls actually are will be beneficial.

For the purposes of this text we have categorized general controls as follows:

* ***control environment***
    - communication and enforcement of integrity and ethical values
    - commitment to competence
    - participation by those charged with governance
    - management's philosophy and operating style
    - organizational structure, assignment of authority and responsibility
    - human resource policies and practice

* ***systems development and implementation controls***.
    - in-house development
    - packaged software
    - programme change controls

* ***access control***

* ***continuity of operations***
    - risk assessment
    - physical security
    - disaster recovery

* ***system software and operating controls***

* ***documentation***

We have not described general controls for a specific size of company (that would be a book in itself!) but have assumed that the company is large enough to have a separate IT department, a data centre, and its own "technical" IT personnel to undertake systems developments and programme maintenance. Obviously if a company does not have a data centre, some of the physical controls will not be relevant, or if a company uses only packaged software, it will not have to worry about certain aspects of systems development, but will have to worry about which packaged software to purchase and who will maintain it.

3. CONTROL ENVIRONMENT

In terms of ISA 315 (Revised), the auditor evaluates the control environment as a component of internal control so you might be wondering why it is part of a general control evaluation. The reason is that the evaluation of the control environment as a component of internal control covers the entire organization (to the extent it affects the audit) whilst the evaluation at general control level, concentrates on the control environment within the IT structures. Of course the evaluation of the control environment within the IT structures is part of the overall exercise, but it has some significant and unique aspects to it.
You should refer to chapter 5 as well.

3.1 Communication and enforcement of integrity and ethical values

* in terms of King III, ethical IT governance must be cultivated and promoted and should align with the ethical culture of the organization.
* a strongly ethical culture is important in an IT department, particularly as IT personnel will have access to confidential and sensitive information, and may also have the opportunity to cause disruption to operations and destruction and unauthorized alteration of data.
* IT management should communicate a code of ethical behaviour, comply with it themselves, and take strong remedial action, which may include dismissal, where integrity and ethical behaviour have been lacking. The potential damage (risk) of engaging or retaining individuals who lack integrity is considerable.

3.2 Commitment to competence

* the demands of many of the jobs in an IT department with regard to skills and knowledge as well as the ability to handle pressure can be considerable
* IT management should be committed to matching these attributes to an individual's job description. Again the consequences of an individual not being able to do his job could be immense. Performance reviews and regular discussions with employees as well as ongoing training demonstrate a commitment to competence.

3.3 Participation by those charged with governance

* in terms of King III, IT governance is the overall responsibility of the board and it should provide the required leadership and direction to ensure that the IT achieves, sustains and enhances the company's strategic objectivity. IT governance is not an isolated discipline
* there should be defined mechanisms for the IT department to communicate with the board and report regularly to it
* the board should appoint an IT steering committee to assist is the governance of IT. A steering committee is a group of people knowledgeable about computers, to whom major issues are referred, e.g. policies, future strategy, IT risk, acquisitions of hardware and software
* the IT department should not be seen as a "separate entity" answerable only to itself.

3.4 IT management's philosophy and operating style

* as with the company's overall control environment, this comes down to the attitudes, control awareness and actions of the IT management. Their actions set the tone of the department and as they lead, so will the employees follow. Their management philosophy and management style must demonstrate, communicate and enforce sound control. For example, a manager who shares his PIN code to gain access to the data centre or spends half the day "surfing the internet", can expect employees to start doing the same and worse, before long!

* very often IT personnel are seen as technical specialists who are more interested in IT and the excitement of its capabilities, than they are in the ″boring″ routine of the company's business. This can lead to a level of disharmony within management, particularly if IT as a department "does its own thing".

3.5 Organisational structure and assignment of authority and responsibility

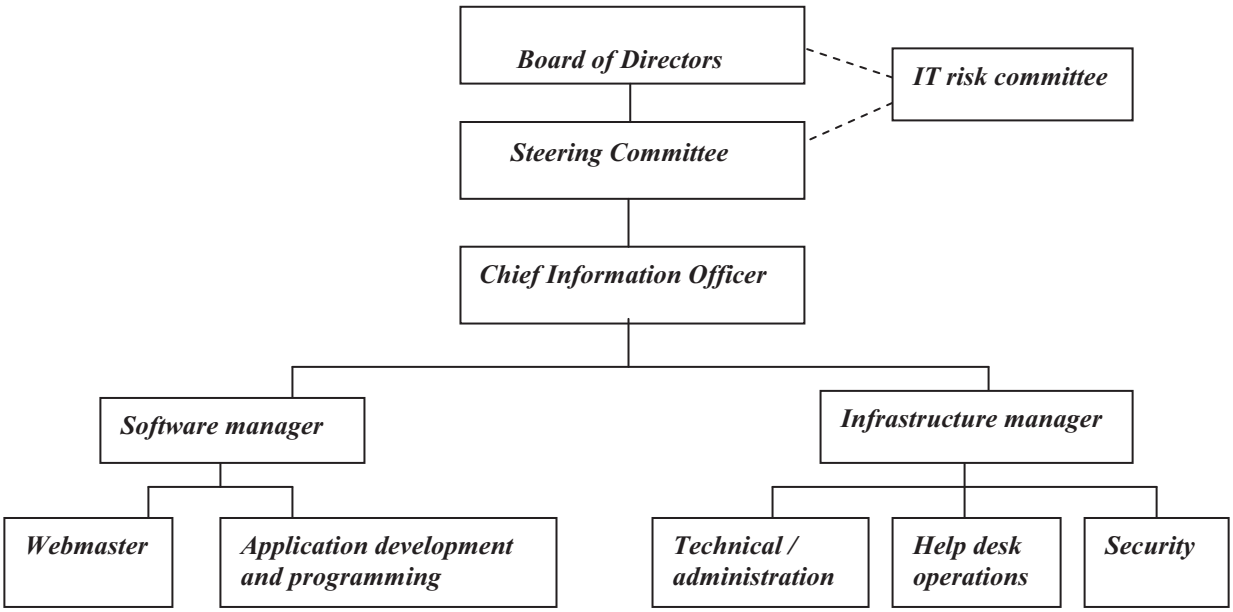
* the organisational structure should achieve two major objectives :
  - it should establish ***clear reporting lines/levels of authority***, and
  - it should lay the foundation for ***segregation of duties*** so that, if possible, no staff perform incompatible functions
* the organisational structure should address segregation of IT and ***user*** departments and segregation of ***duties within the*** IT ***department***

* in terms of King III the chief executive officer should appoint a chief information officer (CIO) who is suitably qualified and experienced. This individual should interact on a regular basis with
  - the board
  - steering committee and audit committee
  - executive management

* overall the functions of supervision, execution and review within the department should be segregated as far as possible

* job descriptions, levels of authority and responsibilities assigned to IT personnel should be documented.

Sound Organisational Structure for an Information Technology Department



Note: There are many variations of organisational structure, e.g. a director may be designated as the CIO and the individual who runs the department may be called the IT manager.

* ***Application development and programming***
- ***Business/systems analysts -*** are responsible for liaising with users to understand their needs and documenting functional specifications for new applications and programme enhancements.
- ***Programmers*** - write the programme code based on the specifications supplied by the business analysts, document the technical specification and debug programmes.

* ***Webmaster*** – many companies now have websites which can be integral to the company's business, e.g. a company trading on the internet. A webmaster should be appointed. Responsibilities will be to
  - design, develop and maintain the company's website
  - regulate and manage the access rights of the users of the site
  - set up and maintain website navigation
  - deal with complaints and other feedback about the site.

* ***Technical/Administration***
  - ***Database administrators -*** have the specialised skills to develop, maintain and manage the database (the store of information),
  - ***Operating System Administrators*** - have the specialised skills to implement, maintain and manage the operating system and hardware,
  - ***Network Administrators*** - have the specialised skills to implement, maintain and manage the company's LAN/WAN etc (refer Ch 9 for further details on these).

* ***HelpDesk/ Operations***
  - ***Helpdesk operators*** - receive calls from users and log their problems/requests on the HelpDesk System, resolve "First Tier" problems where possible (i.e. problems that are easy to solve), as well as performing routine operational duties e.g. checking backups have been completed successfully and managing rotation of backup tapes (see 6.3 for further information on backups).

    Note: "Second Tier and "Third Tier" problems would normally be referred by the HelpDesk to the most appropriate technical administrators/programmers or the vendor concerned.

* ***Security***
  - ***Security personnel*** lay down control procedures for access to all computer facilities, monitor security violations (e.g. logs) and follow these up, issue passwords. The company may appoint an Information Security Officer.

The chart and related job descriptions above, will help to illustrate the following important segregations of duty:

* ***the IT department should be entirely separate from user departments***

  - no transactions should be authorised or executed by any member of the IT department, e.g. placing a purchase order or authorising a wage rate increase,
  - ***no member*** of the IT staff should have access to, or custody of, the physical assets of the company e.g. inventory, or uncontrolled access to the non-physical assets, e.g. the debtors masterfile,
  - IT staff should only be responsible for correcting errors which arise from operating or processing problems; unless in response to authorised requests from user departments for assistance with corrections.

* within the ***IT department*** itself
  - the broad segregations as indicated by the chart, should be implemented,
  - technical administrators should be segregated from programmers and business analysts. Technical administrators have high levels of expertise and although they work mainly with operating systems software, detailed knowledge of the application programmes, would enable them to make unauthorised modifications to the application programmes or data,
  - security functions should be restricted to the security sections, e.g. an operator should not be asked to follow up on logged access violations.

3.6 Human resource policies and practices

Policies and practices for IT personnel will essentially be the same as for other skilled personnel. The IT department will work with the entity's human resource department in respect of these policies and practices. The point has been made several times that an important part of any control system is

"people." The characteristics of honesty, competence and trustworthiness are paramount in a computerised environment and management should institute the following policies and practices:

* proper recruiting policies which include careful checks on an applicant's background and competence,
* immediate exclusion from computer facilities if an employee is dismissed (passwords and user privileges should be cancelled),
* compulsory leave - employees who are involved in unauthorised activity will often be uncovered when they are not present to cover their tracks,
* training and development to keep staff up to date and able to fulfil their functions efficiently and effectively. This should be accompanied by ongoing evaluation of personnel suitability and competence for their jobs and their progress down their career paths,
* written formalisation of human resources policies to provide employees with terms of reference or guidelines,
* rotation of duties - moving employees between functions, is a useful practice as it helps avoid undue reliance on any individuals by ensuring that each employee has a backup . It may also relieve boredom as well as encourage employees to develop new expertise and skills. Rotation of duties should not be implemented to the extent that segregation of duties is compromised, e.g. the computer operator should not be trained as an application programmer and then be placed temporarily in the programming section,
* strict policies pertaining to the private use of computer facilities by IT personnel (and other employees) should be in place, e.g. internet use and running private jobs.

4. SYSTEMS DEVELOPMENT AND IMPLEMENTATION CONTROLS

Systems change because the business world changes, and the need for quicker, different, additional and better quality information increases. Business related systems are said to have a "life cycle", they start, develop, mature and decline. Changes in the company's information system may arise because of changes in the company's business activities, growth, a need to maintain a competitive advantage or just to improve its all round performance by having better information.

Systems development has to do with significant changes relating to computerised systems. This often means that most of the following aspects of the system will be new or significantly changed: hardware, software, communication devices, personnel procedures, documentation, control procedures. One example may be a company which has grown considerably and wants to computerise a previously manual payroll system. Another example may be a company that wants to start selling its merchandise over the Internet to remain competitive. In each case it would probably require new hardware, operating systems, application programmes and procedures to be designed and implemented to achieve these objectives. Unless the entire exercise of designing the system is carefully controlled, the following might occur:

* costs of development may get out of control,
* the system design may ***not*** suit user requirements properly (e.g. important information which is required is not available or is hard for the user to find)
* programmes within the system may contain errors and bugs,
* important financial reporting requirements are not incorporated into the system or are incorrectly understood by the business analyst/ programmer.
* the new system may not incorporate enough controls to ensure the integrity of its programmes and data, e.g. the design of access privileges may give employees write access to files they should not have any access to.
* an excellently designed system may be rendered virtually useless because no-one knows how to use it.
* the information transferred from the old system to the new may be erroneous, invalid or incomplete.

If proper systems development and implementation controls are put in place, the risks mentioned above can be avoided.

4.1 For inhouse development and implementation of systems

4.1.1 Standards

* All systems development should be carried out in accordance with pre-defined standards which have been set for each of the phases described below e.g. components of the ISO 9000 series of standards.
* Compliance with these standards should be strictly monitored and any deviations thoroughly followed up by management.

4.1.2 Project approval

* Projects for systems development may arise out of user requests or as a result of strategic planning.
* A feasibility study should be carried out, culminating in either:
  - a system specification for an in-house development proposal,
  - a proposal which involves the purchase of off-the-shelf software (packaged software),
  - rejection of the project.

  The feasibility study should include a cost/benefit analysis which lists and puts a money value to:
  - all requirements for the project such as personnel, hardware, software and running costs,
  - all benefits arising e.g. increased revenue, reduced costs, improved controls.
* The steering committee should give its approval prior to commencement of the project.

4.1.3 Project management

* A project team should be formed by the steering committee to manage the project and should include IT and appropriate user personnel, including accounting and internal audit personnel.
* The development project should be planned in stages, each stage detailing the specific tasks which must be completed.
* Responsibility for each specific task must be allocated to appropriate staff members.
* Deadlines should be set for completion of each stage and each specific task.
* Progress should be monitored at regular intervals to identify any problems which may affect achievement of goals set - critical path analysis may be useful here.
* Regular progress reports should be submitted to the steering committee.

4.1.4 User requirements

* Business analysts should carefully determine and document all user requirements relating to the system e.g. input, procedures, calculations, output, reports, financial reporting requirements, audit trails.
* Special care should be taken to consult both internal and external auditors as to their requirements and their recommendations concerning internal controls e.g. access controls, validation checks.
* Management of each user department should sign their approval of the specifications recorded to satisfy the needs of their individual departments.

4.1.5 Systems specifications and programming

* Programme specifications should be clearly documented.
* Programming should take place in accordance with standard programming conventions and procedures e.g. for coding, flow charting, programme routines and job control routines.
* Programmers should carry out all programme development in a development environment and should have no access to the live environment.

4.1.6 Testing

* Programme coding of individual programmes should be tested by the programmers using standard debugging procedures like programme code checking and running the programme with test data (***programme tests and string tests***).
* The system should also be tested as a whole to ensure that all programmes are integrating properly - this would normally be done by business analysts in a test environment (***systems tests***).
* The system should also be tested on an output level by management, users and auditors to establish whether the system is satisfying the requirements of its users (***user acceptance tests***).

4.1.7 Final approval

* Results of the above testing should be reviewed by all involved to ensure that necessary changes have been made and errors corrected.
* The project team should then obtain final approval from the board, users, internal audit and IT personnel before going ahead with conversion procedures.

4.1.8 Training

* A formal programme should be devised setting out in detail all personnel to be trained, dates and times for their training and allocating responsibility for training to specific, capable staff.
* User procedure manuals and updated, clearly defined job descriptions should be compiled and used in the training exercise.

4.1.9 Conversion

Controls are necessary at this stage to ensure that programmes and information taken onto the new system are ***complete***, ***accurate*** and ***valid***:

conversion project: the conversion should be considered as a project in its own right, applying the principles explained in (4.1.3) above.

data cleanup : data to be converted must be thoroughly checked and discrepancies resolved prior to conversion. For example, if a new inventory application is being introduced, physical inventory should be counted so that correct quantities can be entered onto the system.

conversion method: the conversion method must be selected:

- parallel processing of the old and new systems for a limited period, or
- immediate shut-down of the old system on implementation of the new system, or
- conversion of the entire system at one time or
- phasing in different aspects over a set period.

preparation and entry: controls over preparation and entry of data onto the new system should include the use of a data control group to:

- perform file comparisons between old and new files and resolve discrepancies,
- reconcile from original to new files using ***record counts*** and ***control totals***, e.g. if there were 300 employees on the old payroll, there must be 300 employees on the new payroll
- follow up exception reports of any problems identified through use of programmed checks e.g. no employee identity number.
- obtain user approval for data converted in respect of each user department.
- obtain direct confirmation from customers or suppliers of balances reflected on the new system.

4.1.10 Post-implementation review

Users, IT personnel and auditors should review the system several months after implementation to determine whether :

* the system is operating as intended (all bugs resolved),
* the systems development exercise was effective, (for future reference),
* all aspects of the new system are adequately documented in accordance with predetermined standards of documentation.

4.1.11 Documentation

* the project itself and all the activities which took place in the planning and execution of the project should be documented.
* documentation relating to the system itself, must also be prepared, e.g. systems analysis, flowcharts, programming specifications, etc.
* documentation should be backed up on an ongoing basis and stored offsite.

4.2 Systems development and implementation based on packaged software

When a company decides that it needs a new system, one of the options it has, is to purchase packaged software as opposed to developing the software itself (in-house). This is not just a matter of buying a package, installing it and away you go – the majority of the systems development and implementation controls covered above will apply. The major difference between inhouse developed and packaged software is that for purchased packages, the company will have no control over the specifications and development, e.g. writing the programmes, or testing of the software. Purchased packages are designed to meet the generic requirements for lots of users with similar needs and although current packages contain hundreds of features and capabilities, the user basically gets what the package offers, nothing more and nothing less. This means that from the company's perspective, the emphasis will be deciding whether the package offers features and capabilities which match with what the company's users want.

4.2.1 the advantages of packaged software

* lower cost
* the entire software development project is completed far quicker because development and testing have been done on the software by the developers
* the package can be demonstrated up front, so IT personnel and users can see what the package "can do". Sample reports can be examined and the computer capabilities required by the software can be determined and tested
* technical support (by phone or over the internet) is usually available from individuals who are very skilled and knowledgeable about the specific package, and comprehensive manuals are supplied
* software companies usually upgrade the packages on an ongoing basis.

4.2.2 the disadvantages of packaged software

There are not too many disadvantages. This is mainly because the software development industry is highly competitive which has resulted in an explosion of packages on the market covering virtually every industry. The packages are of high quality, fully debugged and very reliable. The major disadvantages are that

* the package may not meet the company's requirements exactly
* excellent software developed overseas may, for example, not satisfy South African tax or financial reporting requirements (many of these packages do offer SA versions)
* changes can't be made by a purchaser of the software.

Of course there are packages available which are of a lower quality, short on control features and not particularly reliable which give rise to plenty of disadvantages, but the project team will endeavour to avoid these packages.

4.2.3 summary of controls for the acquisition and implementation of packaged software

* ***project management*** – the entire exercise should be run as a project by a team appointed by the steering committee

* ***project approval*** – a feasibility study must still be conducted to determine
  - user needs
  - specifications (capabilities, functions, controls, ease of use) of packages available in the market
  - costs and benefits (costs will include costs of the package itself, running it, appointing and training staff, purchasing additional hardware, etc)
  - technical support and reliability of the supplier
* ***approval*** for the package chosen should be obtained from users, internal audit and the steering committee, and authorization for its purchase should be obtained from the CIO and the board.
* ***training*** – all affected IT personnel and users should be trained in the use of the new software
* ***conversion*** – moving data onto the new system should be controlled as explained under in–house development
* ***post implementation review*** – again IT personnel, users, internal audit, should review the new software several months after implementation to determine whether it is operating as intended
* ***documentation*** – the systems documentation, user manuals, etc, will come from the supplier but the planning and execution of the project itself should be documented.

4.3 Programme change controls (also referred to as programme maintenance)

When a new system is developed and subjected to vigorous systems development controls, the result is usually a well designed, effective application which produces reliable information in a format which satisfies the user. However, this is just a starting point. There is virtually always an on-going need to modify applications to meet changes in user requirements, improve ways of presenting information and so on. These modifications require changes to the application programme and if such changes are not carefully controlled, unauthorised modifications could be made negating the effect of the strong controls which were implemented when developing the system. Programme changes of an ongoing nature are usually referred to as programme maintenance. The controls which should be in place, are:

* programme change standards similar to those for systems development must be adhered to

* requests for programme changes should be documented on prenumbered, preprinted change control forms and listed in a register

* programme change ***requests*** should be evaluated and approved by:
  - the user department (application changes)
  - the IT manager (CIO) (application and systems changes) and
  - steering committee for more major changes

* programme changes should be effected by programmers - not operators or users (in some systems programme changes can be made by a user from his workstation, this system would have to be carefully controlled primarily by written approvals, access controls, logging by the computer and review thereof)

* any major change should be managed as a mini project (see systems development)

* changes should be made to a development programme not the production programme (i.e. to a ***copy*** of the live programme)

* changes should be tested by the programmer and an independent (senior) programmer using standard debugging techniques

* programme changes should be discussed with users and internal audit and they should sign the change control form if they approve

* all documentation affected by the change should be updated and the entire change exercise itself should also be documented

* the amended programme should be copied to the live environment by an independent technical administrator, and all programme changes should automatically be logged by the computer

* the IT manager should review the log of programme changes and reconcile it to the programme change forms and register.

5. ACCESS CONTROLS

5.1 Introduction

There is an old saying that prevention is better than cure, and it is very applicable to computerised systems. The consequences of unauthorized access to a system can be disastrous for a company; uncontrolled physical access to the hardware has resulted in the theft of, or damage to, expensive equipment ***and*** the data which will be stored on the hardware. Unauthorised logical access (which really means gaining unauthorized access to data, and programmes electronically stored through a workstation/terminal) can result in the destruction of data, the manipulation of data or the theft of data and programmes. Rather than having to implement a "cure" for the theft, destruction etc, it is far better for the company to prevent these very negative consequences, by implementing strict access control policies and procedures. Again, computer security is a huge and very complex topic which exercises the minds of the best and brightest. Many companies are permanently under siege from "hackers" trying to break into their systems, sometimes with very malicious intent and at other times "just for the challenge", or so they say! Measures to prevent/minimize the negative consequences of terror attacks, natural disasters, etc, must also be implemented. All of these preventative measures must take into account the important fact that authorized employees must still have access to the hardware, programmes and data they require to do their jobs effectively and efficiently.

Access to all aspects of the system must be controlled:

* hardware,
* computer functions at system level, (accessing the computer system itself)
* computer functions at application level, (accessing a specific application or module within an application)
* data files/databases,
* utilities,
* documentation (electronic or hard copy),
* communication channels.

5.2 Security policy

A security policy addresses the security standards which management need to achieve to maintain the integrity of the company's hardware and software. Once management have decided what it is they want to achieve, they can go about implementing the policy. The policy should be documented and should be based on principles rather than detailed procedures. Important principles include:

* ***Least privilege*** - employees should be given access to only those aspects of the system which are necessary for the proper performance of their duties, e.g. a clerk in the wages department should not be given access to inventory records as he does not "need to know" what is contained in the inventory records. On a more general level, employees who do not need any access to perform their functions, should not be given any access, e.g. a factory worker needs no access privileges to the company's systems.
* ***Fail safe*** - this principle requires that ***wherever possible***, if a control "fails", whatever is being protected by that control, should remain "safe", e.g. if logical access control software malfunctions, the system should shutdown completely, rather than allowing uncontrolled access. The same principle will apply to physical controls.
* ***Defence in depth*** - this means that protection is not left up to one control only, but rather to a combination of controls

* ***Logging*** - adherence to this principle, requires that the computer's ability to log (record) activity which takes place on it, should be extensively incorporated, e.g. unsuccessful attempts to access the system should be logged and followed up. Logging is ***not*** an effective control activity, ***unless*** the logs are regularly and frequently reviewed ***and*** follow up action taken where control violations are identified.

Access controls will vary considerably depending on the size of the company, the extent of its computerization, and how it is set up. Access controls at a bank or multinational company are going to be different to a small or medium sized company but the principles remain the same.

5.3 Physical access control

A large company will have extensive equipment, e.g. CPU, servers, secondary storage devices, etc, which will normally be housed in a ***data centre***. It will also have hundreds of microcomputers, printers, etc, in user departments on LANs and WANs. A smaller company could just have a small number of microcomputers (which could be "stand alone" or networked) and a printer. Despite the fact that the consequences of unauthorized access may be far greater for a large company in absolute terms, in relative terms unauthorized access may be equally devastating for a smaller company. The point is that access control is important to all businesses, but how physical access is controlled will vary considerably.

A combination of the following physical controls will be implemented to prevent unauthorized entry to an IT data centre (which could of course be part of a large IT department). For example, the IT department as a whole, could be contained in a separate building or wing of a building. All IT personnel would have their offices in this building. The building would also have a ***dedicated room*** in which all the equipment which runs the system would be housed, e.g. CPU, servers, routers, to run the company's systems. This dedicated room would be the data centre. The data centre would not double up as offices although IT personnel would need to go in to perform some of their functions. In this type of arrangement, access to the IT building (or wing) may be controlled and further access to the data centre itself would be far more strictly controlled. Only a limited number of personnel need access to the data centre itself whilst many more need access to the IT department. To put the following physical controls into perspective, think about how important it is to a bank to protect its entire system.

* ***visitors from outside the company to the IT building should***
  - be required to have an official appointment to visit IT personnel working in the IT department, e.g. external maintenance personnel
  - on arrival be cleared at the entrance to the company's premises e.g. by a phone call to the IT department
  - be given an ID tag and possibly escorted to the department
  - not be able to gain access through the locked door (must "buzz")
  - wait in reception (or be met at the door) for whoever they have come to see
  - be escorted out of the department at the conclusion of their business.

* ***company personnel other than IT personnel***
  there should be no need for other personnel to enter the ***data centre*** and access to the IT department should be controlled in a practical manner as there will be contact between the IT department staff and users on a regular basis.

* ***physical entry to the data centre*** (dedicated room)
* only individuals who need access to the data centre should be able to gain entry
* access points should be limited to one
* access should be through a door which is locked other than when people are entering or exiting, i.e. not propped open by a wastepaper basket for people to come and go
* the locking device should be de-activated only by swipe card, entry of a PIN number, scanning of biometric data, e.g. thumbprint
* entry/exit point may be under closed circuit TV

Remember the data centre is the heart of the company's information system.

* ***remote workstations/terminals***
in most businesses, workstations/terminals are distributed around the offices, so centralized control measures are not possible (other than where say, a group of telesales operators are sitting in a separate room). Some physical controls will still be implemented. Terminals
  - can be locked and secured to the desk
  - placed where they are visible and not near a window
  - offices should be locked at night and at weekends.

5.4 Logical access controls

Logical access controls will be primarily ***preventive*** i.e. designed to prevent unauthorised access via terminals, but these will be supported by logs which are ***detective*** in nature e.g. logging of attempted access violations as well as logging authorized access. Logical access control also plays a big part in controlling access at application level, but is dealt with under general controls because before any transaction processing takes place, access controls must be implemented as part of the general controls framework. Logical control access is also covered in the section on application controls.

Against the overall backdrop of ensuring that ***only authorized individuals*** are able to gain access to the facilities on a ***least privilege/need to know basis*** i.e. access is given only to those aspects of the system which are necessary for proper performance of their duties, the following controls in various forms can be implemented through the access control software and other programmes

* ***identification*** of users and computer resources
  - Users, some examples
    - user identification, (User IDs)
    - magnetic card or tag
    - biometric data e.g. thumbprint, facial recognition
  - Terminals, some examples
    - terminal identification (system recognizes terminal ID number or name)

* ***authentication*** of users and computer resources

  Authentication of the user is used to verify that the ***user*** of an ID is the ***owner*** of the ID. Authentication can be achieved in various ways:
  Users, some examples
  - entering a unique password
  - entering a piece of information which an unauthorized individual would not know about the genuine user, e.g. great grandmother's first name. This works on the same principle as a password. The information, say 10 different pieces of information, is held on the system (securely) as provided by the user. When the user ID is entered, the system selects one piece of information and poses a related question to the user. If the answer keyed in is correct, authentication has been achieved. It is also possible that a single piece of information is stored but regularly changed.
  - connecting a devise to the USB port of the terminal, e.g. to authenticate the authorization and release of an electronic funds transfer, a leading bank requires that the authorized employees have a devise called a "dongle" which must be inserted before the payment can proceed. This works in combination with a password and both are unique to the user. The password and dongle are needed to authenticate the user. Another bank uses a small random number generator devise which produces a number which must also be used in conjunction with the password. It is really a second unique password. In a company a "one time" password can be generated on a server and sent by SMS to the user. It is the same principle. A combination of the above techniques is called multi-factor authentication and is used where very strict access control is required. The

dongle will only work on a terminal on which the bank's specific software has been loaded, this is a form of terminal authentication.

The fact that a user ID can be linked to the individual, is a strong isolation of responsibility control.

* ***authorisation,*** this is defining the levels (types) of access to be granted to users and computer resources

  - once the system has authenticated the user, access will only be given to those programmes and datafiles to which the user is ***authorized*** to have access, and as pointed out, this should be only to programmes and data the user requires to do his job. Users can be given different levels of authority
  - users, some examples
    - a user may be granted read only (this means a file can only be read) or
    - read and write (this means a file can be read and written to, e.g. the user can add, create, delete).
  - terminals, some examples
    - although modern software concentrates access privileges around the user, specific terminals can be linked to specific applications e.g. warehouse terminal not linked to the wage application, or to the EFT facility
    - restricted hours of operation e.g. terminal shuts down at 4pm and comes on at 7 am.

* ***logging,*** this is recording access and access violations for later investigation.
  An access log records who accessed the system and by comparing it to some other piece of information, may provide evidence of unauthorized access. For example, if Willy Worker is logged as having gained access to the system on June 10, when he was supposed to be on holiday, then there is something strange going on!
  Logging and follow up is essentially a detective control. The emphasis on access control will be on preventing unauthorized access, but logging and follow up is still an essential control.

* ***Access Tables***
  The computer cannot perform logical access control unless a large number of details are defined in tables to which the system can refer. These tables identify all "objects" and "conditions" which the computer has to "know" in order to be able to control access. These objects include :
  - all authorised PCs (PC IDs),
  - all authorised users (user IDs),
  - all passwords,
  - all programmes,
  - all possible modes of access (no access, read-only, read and write), time of day (e.g. a bank teller may only be able to log in between 8.30 am and 4.00 p.m.), etc.

Setting up these tables is not technically difficult for a skilled person, but requires meticulous care. Broadly, it happens as follows: when a new employee joins say, the payroll department, he will need access to files etc which are required to do his job. This detail is provided by the manager of the payroll department on a written form which describes exactly what the employee's job description is. For example, the employee must be able to read the employee masterfile and change some fields and not others; he may need to be able to change an employee's address but not the wage rate field. This and everything else the employee must be able to do, has to be reflected in the employee's user profile and is related to the access tables.

It is now possible to compile the necessary tables and the user profile which specifies which combinations of these objects and conditions should be allowed/authorised and which combinations should be disallowed (access violations). These profiles should be determined by

the IT manager and senior IT staff working in conjunction with senior user personnel and system design documentation. A simple example will illustrate user profiles :

Fred Bloggs the storeman, is to be given access to the inventory masterfile, but this is to be "read only" access. He has a user identification and a password. For simplicity sake, we will say that Fred Bloggs needs no access to any other data programmes. Once Fred Bloggs' needs have been established, senior IT staff will create Fred Bloggs' "user profile", which will be stored in a secure file on the system. The computer now has something to refer to. When Fred Bloggs activates his PC, he will be prompted to enter his User ID and password. The computer will check against the access table whether Fred Blogg's PC and his user ID are listed (identified). The computer will check that Fred has proved who he is by matching Fred's password to listed passwords in the access tables (authentication). If Fred has entered his password correctly, the computer will "fetch/consult" Fred's user profile and display the inventory application functions to which he has access. The computer may also check that Fred is at a PC which has authorised access to the inventory application. Fred may now call up the inventory masterfile but if he tries to write to that file, the computer will check against his profile and prevent him from doing so as he has "read only" access.

Access profiles like the one described above, are usually set up for "user groups" rather than for individual users, as this is a more efficient way of controlling access. In other words, management would determine what access privileges a storeman should have and Fred Bloggs would then be allocated to the "storeman user group". If you imagine that Fred's company may have five hundred stores around the country, each with one storeman, it is easy to appreciate that it would be more efficient to define one group profile and allocate all 500 storemen to that group, rather than having to define access separately for each user.

If Fred Bloggs attempts to get into an application or module, or exercise a privilege he does not have, the computer will send him a screen message, and he will not be able to proceed (or the computer may just fail to respond). The system may also be set up in such a way that what appears on Fred Bloggs' screen may not give him the option to click onto what he wants to do. For example, if he is not allowed give approval, there will be no approval field for him to click on.

* ***Controls over passwords.***

The strict control of passwords is fundamental to successful, logical access controls

- passwords should be unique to each individual (group passwords should not be used).
- passwords should consist of at least six characters, be random not obvious, and a mix of letters, numbers, upper/lower case and symbols.
- passwords/user-IDs for terminated or transferred personnel should be removed/disabled at the time of termination or transfer.
- passwords should be changed regularly and users should be forced by the system, to change their password (system sends the user a screen message to change his password and allows a limited number of attempts to enter his existing password. After this, access will not be granted until a new password has been registered).
- the first time a new employee accesses the system, he should be prompted to change his initial password.
- passwords should not be displayed on PCs at any time, be printed on any reports or logged in transaction logs.
- password files should be subject to strict access controls to protect them from unauthorised read and write access. Encryption of password files is essential.
- personnel should be prohibited from disclosing their passwords to others and subjected to disciplinary measures should they do so.
- passwords should be changed if confidentiality has been violated, or violation is expected.
- passwords should not be obvious, e.g. birthdays, names, name backwards, common words, and should not be the same as the user ID.

5.5 Other access control considerations

* ***Data communication***

Data communication relates to the transmission of information from a sender to a receiver in electronic form. Information must be sent down a link which may be a ***fixed line***, e.g. a public telephone network, or a dedicated line linking two computers, or a ***fibre optic*** cable, or by ***wireless*** technology, e.g. satellite transmission, cellular telephones or even cordless computer devices, such as a cordless mouse. All of these transmission media are used in business and are really the domain of the computer and telecommunication expert.

However, because they do form an integral part of information systems used in business, the general auditor needs to have a broad understanding of how they work and must realize that they do present an opportunity for an unathorised person to access the system. Control is achieved by

- the implementation of specialized software which is responsible for:
  - controlling access to the network
  - network management (i.e. controlling traffic flow, routing data to its destination and logging network activity)
  - data and file transmission (controls the transfer of data and files e.g. making sure the entire message is delivered)
  - error detection and control (identifies errors which indicate that the data received is the same as the data sent)
  - data security (which protects the data from unauthorized access during transmission)
- encryption (converting data into a secret code) of data which is being transmitted
- the protection of physical cabling (under the control of the client) e.g. channelled within brickwork, under the floor etc. The use of fibre optic cable is far more secure than traditional wire cabling but far more expensive. Wireless communications can be a real threat to a company and controlling access in this environment has taken on far greater significance.

* ***Firewalls***

Once a company's network is connected an to external network such as the internet there is an increased risk of unauthorized access to the company's network. A firewall is a combination of hardware and software that sits (probably in the data centre) between the company's network and the external network. They operate as access control gateways which restrict what traffic can flow in and out. This could be as detailed as the prevention of incoming transmissions from undesirable sites and will include anti virus software and intrusion detection software (which detects malicious behaviour such as the presence of "worms") and alerts the company to it. Firewalls should be tested regularly, make use of the "most up to date" software, and warnings etc, must be logged and followed up.

* ***Libraries***

In a computer environment, libraries may be both in electronic form (on the system) and in physical form. Either way, access to the information in the library must be protected. This is done in the conventional way e.g. library software will protect back up, copies of programmes from unauthorized changes being made, record (log) any authorized access, audit changes and monitor users. A physical library which may contain documentation relating to the system and data stored on discs and tapes or other mobile storage devices should be

- physically access controlled and
- the information on the storage device could also be password protected and
- issue (of items) from the library should be authorized and recorded
- externally labelled.

* ***Root access/system wide access/super-user privileges***
  This level of privilege gives the user concerned virtually unlimited powers to access and change, without trace, all programmes and data, bypassing normal access controls, and therefore should only be given to a very limited number of IT personnel.

* ***Utility programmes/ Database access***
  Access to utility programmes and high level access directly to the database provides the potential to change/delete data and programmes without leaving an audit trail (normally changes/deletions are made through application programmes which ensure that such activities are subject to all the normal access controls, including automatic logging). For example, a debtor's balance may be altered (reduced) without trace using this type of programme, whereas a debtors balance should normally only be reduced by a payment being processed or an authorised credit note being passed using the application software.

5.6 Supplementary access controls

* Automatic account lock-out, in the event of an access violation e.g. incorrect password entered more than three times.
* "Time-out" facilities which automatically log out the user from the system, if a period of more than (say) three minutes expires during which there has been no activity.
* Automatic logging, review and follow up of access and access violations.
* Encryption of confidential and critical information.
* Sensitive functions and facilities can be afforded extra protection by requiring two or more passwords in order to gain access.
* Additional one-off passwords can be given to supplement an existing user ID and password to protect sensitive transactions such as a transfer out of a bank account. For example, when a user wants to make the transfer the system automatically generates a unique password and sends it to the user's cellphone for that user to enter. The assumption is that somebody trying to use another person's user ID and password (which they have obtained by devious means), will not have the genuine user's physical cellphone and therefore will not receive the necessary one off password. The genuine user will also be alerted to the fact that someone is trying to transfer money out of their account.

6. CONTINUITY OF OPERATIONS

These controls are aimed at protecting computer facilities from natural disasters (e.g. flooding or fire), as well as from acts of destruction, attack or abuse by unauthorised people. Poor controls result in "down time" and disruption to normal processing. Although South Africa has reasonably stable weather conditions, floods and fires and other natural disasters do still occur. Our high crime rate and general unrest, places businesses at risk of armed robbery and damage from explosion.

6.1 Risk assessment

Although the company's risk assessment procedures are regarded as a separate component of internal control and will be evaluated by the auditor as a component, a general control evaluation should consider the company's risk assessment procedures to the extent that they relate to IT risk (which as previously stated, is regarded by King III as a major risk facing companies). The dependence by large companies on their IT systems is huge and failure to assess and address IT risk threatens the continuity of operations. The auditor will evaluate whether

* assessing IT risk is an integral part of the company's risk assessment procedures
* there is an appropriate level of experience and knowledge with regard to IT risk on the risk assessment committee
* the risk committee meets regularly but is available to deal with the threat of unexpected IT risk on an ongoing basis
* the risk assessment committee recognizes and assesses all types of threat relating to IT which could disrupt operations including e.g.
  - fraud and theft perpetrated through the IT system
  - physical and infrastructure damage

- hacking and viruses
- non-compliance with IT laws, rules, standards and best practice

* accepted risk assessment protocols (ways of doing things) are followed
* assessments are documented and reported to the board
* responses to risks are recorded, implemented and monitored.

6.2 Physical security

These controls are designed to ***protect*** facilities against natural and environmental hazards and attack or abuse by unauthorised people. The following pertain more specifically to the ***data centre***

* physical location (site selection)
  - the data centre (and obviously the building in which it is housed), should be placed away from obvious hazards e.g. river banks, main traffic areas, the factory, stores of hazardous materials
  - the facility should be located within a secure area within a building i.e. no outside walls and windows
  - there should be a secure door and access control devices
* fire and flood
  - automatic gas release (e.g. CO2), smoke detectors, fire extinguishers, no smoking allowed
  - situated above ground level and away from water mains
  - raised flooring in the data centre.
* power surges
  - use of "uninterrupted power supply" equipment and back up generators, particularly if continuity is critical (normally is)
* heat and humidity
  - air-conditioning preferably on its own electrical circuit
* physical access controls - see discussion under access controls (5.3).

6.3 Disaster recovery

These are controls implemented to minimise disruption as a result of some disaster which prevents processing and/or destroys/corrupts programmes and data.

* a disaster recovery plan
  - a written document which lists the procedures which should be carried out by each employee in the event of a disaster,
  - the plan should be widely available so that there is no frantic searching if a disaster occurs. Time is usually precious,
  - the plan should address priorities i.e. The order in which files or programmes should be reconstructed, with the most important being allocated the highest priority, as well as where backup data, programmes, hardware etc may be obtained,
  - the plan should be tested,
  - the plan should detail alternative processing arrangements which have been agreed upon in the event of a disaster, e.g. using a bureau
* backup strategies
  - backups are copies of all or parts of files, databases, programmes taken to assist in reconstructing systems or information, should they be lost or damaged,
  - back up of all significant accounting and operational data and programme files should be carried out frequently and regularly,
  - at least three generations of backups should be maintained (grandfather, father, son),
  - the most recently backed up information should be stored off-site,
  - all back up should be maintained in fireproof safes and on-site back ups should be stored away from the computer facilities,
  - critical data and programmes can be copied in real time to a "mirror site", so that it is possible to switch processing to the mirror site in the event of a disaster. For

example, a large refinery in KZN duplicates its processing on a second computer installation housed in a separate, very secure (bomb proof as well) site on the premises. Obviously this is expensive, but the computer system is an integral part of both operations and record keeping, and a refinery is a potential target for terrorist attack. The economy would suffer if the refinery could not operate because its computer systems were non-functional,

- copies of all user and operations documentation should be kept off-site.

6.4 Other measures

There are a number of other control measures that can be taken which will assist in preventing or alleviating disaster:

* applying the concept of redundancy (simplistically this means having a "spare" as a back up) e.g. the use of dual power supplies, or as explained above, mirroring
* regular maintenance and servicing of equipment to prevent failure
* adequate insurance cover to provide funds to replace equipment
* avoidance of undue reliance on key personnel by maintaining complete and appropriate documentation and by training of understudy staff, e.g. the disaster recovery plan should not revolve around one staff member
* arrangements for support to be provided by suppliers of equipment and software, who may even provide alternate processing facilities
* the use of fire walls and use of anti virus software.

7. SYSTEM SOFTWARE AND OPERATING CONTROLS

System software controls the use of the hardware and the use of the application and end-user software, as well as other resources on the system. The evaluation of system software is very much the domain of the computer audit specialist with good technical knowledge. Systems software is made up of various kinds of software including, inter alia

* ***Operating system software which***
  - controls the use of the hardware
  - tests critical components of the hardware and software where the computer is started
  - controls the input and output of data
  - schedules the use of resources and programmes. Think of it like this : in a business environment, there are hundreds of transactions going on all the time, from different parts of the business. Transactions are put in queues because they can't all be dealt with at once, especially as lots of things may be happening at the same time; input instructions may be coming from one programme, output from another and so on. The operating software makes sure that all this happens in an efficient and orderly manner
  - monitors the activities of the computer and keeps track of each programme and the users of the system
  - provides the interface with the user, e.g. how the user communicates with the computer

* ***Network management software*** which enables computer systems to communicate with each other

* ***Database management software*** which enables the user to create, maintain and use data files in an efficient and effective manner

* ***System development software*** which is used to develop new software, e.g. assemblers, compilers

* ***System support programmes*** such as anti-virus software, data compression software, etc.

A vitally important part of any IT department is to make sure these programmes (software), operate as they should and system software controls are aimed at monitoring the system. Operating controls are the policies and procedures which should be in place to work with the system software controls to make sure the computer system (the hardware and software), run like a "well oiled machine". Controls include

* Operating policies and procedures which are fully documented, regularly reviewed and updated
* System software which maintains a log of activity on the system detailing all activity which had taken place, including
  - hardware malfunction
  - intervention by personnel during processing
* Skilled technicians who can resolve operating problems for users
* Adherence to international system software control protocols (how things are properly done)
* Follow up on access violations, attempted violations
* Follow up of potential virus infection
* Adherence to manufacturers' equipment, maintenance and usage guidelines
* Strict supervision and review of IT employees (IT manager needs to know what his staff are doing)

8. DOCUMENTATION

8.1 Introduction

Sound documentation policies are essential, because documentation can be critically important in:

* improving overall operating efficiency,
* providing audit evidence in respect of computer related controls,
* improving communication at all levels,
* avoiding undue reliance on key personnel,
* training of users when systems are initially implemented.

There are two major objectives to bear in mind regarding documentation:

* all aspects of the computer system should be clearly documented,
* access to documentation should be restricted to authorised personnel.

8.2 Documentation standards

As for all other aspects of the computer environment, pre-determined standards should exist for documentation and adherence thereto should be enforced. These standards should require at least:

* general systems descriptions,
* detailed descriptions of programme logic,
* operator and user instructions including error recovery procedures,
* back-up and disaster recovery procedures,
* security procedures/policy,
* user training,
* implementation and conversion of new systems.

This documentation should be promptly updated for any changes and responsibility for this task should be allocated to specific individuals (isolation of responsibility).
Back-up copies of all documentation should be stored off-site.
Access to documentation should be restricted to authorised personnel

APPLICATION CONTROLS

1. DESCRIPTION

1.1 An ***application*** is a set of procedures and programmes designed to satisfy all users associated with a specific task, for example, the payroll cycle. Other examples include making sales, placing orders with suppliers and receiving or paying money. Application controls are very closely linked to the cycles described in Chapters 10 to 14.

1.2 An ***application control*** therefore is any control within an application which contributes to the accurate and complete recording and processing of transactions which have actually occurred, and have been authorised (valid, accurate and complete information).

1.3 The stages through which a transaction flows through the system can be described as ***input, processing*** and ***output*** and application controls can be described in terms of these activities, e.g. an application control relating to input.

1.4 In addition to implementing controls over input, processing and output, controls must be implemented over ***masterfiles***. A masterfile is a file which is used to store only standing information and balances, e.g. the debtors masterfile will contain the debtors name, address, contact details, credit balance, and the amount owed by the debtor. The masterfile is a very important part of producing reliable information and must be strictly controlled. For example, if a salesperson wants to make out an invoice for a credit sale on the system, the first thing he will do is enter the customer's name or account number to see if the customer is a valid customer. The system checks the account number (or name) against the ***masterfile*** and if there is no match, the salesperson cannot proceed. If the customer is a valid customer, the order can be taken, but the system will automatically check the total value of the goods bought against the customer's ***credit limit*** on the masterfile and if the limit has been exceeded, the sale will not be permitted until it has been cleared (approved) by the credit controller. This illustrates the importance of protecting the ***masterfile***. If the debtors masterfile is not protected, unauthorized changes to it could be made, e.g. a customer who has not been checked for creditworthiness could be added, or a credit limit could be changed, resulting in losses from bad debts. Controls over the ***masterfile*** are application controls and are referred to as masterfile maintenance controls.

1.5 The objective of controls in a computerised accounting environment is generally regarded as being centred around the occurrence, authorisation, accuracy and completeness of data and information processed by and stored on the computer.

occurrence and ***authorisation*** are concerned with ensuring that transactions and data:

* are not fictitious (they have occurred) or fraudulent in nature, and
* are in accordance with the activities of the business and have been properly authorised by management.

a*ccuracy* is concerned with minimising errors by ensuring that data and transactions are correctly captured, processed and allocated.

c*ompleteness* is concerned with ensuring that data and transactions are not omitted or incomplete.

It follows therefore that application controls can be further classified in terms of input, processing and output, e.g. authorisation controls over input, authorisation controls over processing, completeness controls over input, completeness controls over processing and so on. However, this can be confusing and over analytical particularly because in current computerised systems input, processing, and output are merged into one. It is more important to understand what the control does and how it is carried out. If you understand that, you will understand the objective of the control.

1.6 As we noted earlier in this text, ***preventing*** errors from entering the system is far better than ***detecting*** them later on. However, systems are not perfect so, whilst the main focus of

application controls will be on prevention of errors, a good system will also have strong detection controls. If errors are detected, they must be ***corrected*** so there will be correction controls for correcting errors which have been identified by the detection controls.

2. UNDERSTANDING CONTROL ACTIVITIES IN A COMPUTERISED ACCOUNTING SYSTEM

This section is structured as follows:

2.1 Introduction
2.2 Segregation of duties
2.3 Isolation of responsibilities
2.4 Approval and authorisation
2.5 Custody
2.6 Access controls
2.7 Comparison and reconciliation
2.8 Performance reviews.

2.1 Introduction

Before moving on to discussing specific techniques in the next section of the chapter, we will discuss the control activities identified in Chapter 5 and referred to in ISA 315 (Revised) in the context of a computerised system. This will give you a better understanding of how control techniques and specific application controls are implemented.

It is also important to remember that application controls are a combination of manual and automated (programme) procedures. We can also refer to manual controls as ***user controls*** and they include all the controls which ***people*** carry out, e.g. signing a cheque, authorizing a document, performing a reconciliation, checking goods delivered by a supplier against the delivery note, etc.

2.2 Segregation of duties

In a manual system, segregation of duties is achieved by assigning incompatible functions to different individuals. This facilitates the checking of one employee's work by another employee and prevents an employee from covering up errors, unauthorized actions and misappropriations, e.g. theft.

Potentially, computerisation is a danger to segregation of duties as it takes employees out of the system and enables the control procedures relating to authorising, executing, custody and recording to be performed by one employee and his computer. In addition, computerisation enables numerous employees to gain legitimate access to the accounting records, which means that the risk that they may be performing incompatible functions is increased. For example, the storeman who has custody over physical inventory, may have a PC which links him to the inventory masterfile, so that he can access these records to instantly get information about inventory on hand. He therefore has custody of the asset and access to the asset records. This is poor internal control unless he is strictly denied the ability to ***change*** the inventory records.

Segregation of duties in a computerised environment is achieved primarily by controlling access which employees have to the system itself, the applications on it, and the modules or functions within the application. This is achieved by setting up user profiles on the system for each employee which detail exactly what that employee must be given access to and what he can do when he has access, e.g. read a file, write to a file, make an enquiry, authorise a transaction, etc

For example, an order clerk will be allowed (by his user profile) access to the module to create an onscreen purchase order, but his profile will not allow him to approve the purchase order. This must be done by his supervisor, whose user profile gives him that ability/privilege. See "approval" (2.4) for an explanation of how this is achieved.

The access to programmes and files granted to an employee is based on the user's functional responsibility.

2.3 Isolation of responsibilities

In a manual system, isolation of responsibilities is usually achieved by making a specific employee (or employees) responsible for each function or procedure and requiring that the employee sign the document relevant to the procedure he is performing, to acknowledge (take responsibility for) having carried out the procedure.

A computerised system can enhance isolation of responsibility by programming the computer to produce a log of who did what and when they did it. If the log is properly followed up it becomes an effective way of isolating responsibility. For example, a company which has five receiving clerks recording deliveries of goods from suppliers with only two PCs available in the receiving bay can, by requiring the use of unique user IDs and passwords, record the identity of the receiving clerk who actually recorded the delivery, and in doing so, isolate responsibility to that person. Of course access controls also contribute to isolation of responsibility – terminal identification and authorization controls as well as user IDs and passwords can restrict (isolate) access to the goods receiving module to terminals in the receiving bay and receiving clerks respectively. Another example: restricting access to the module which facilitates on-screen approval of a credit sale (customer order) to the credit controller, isolates the responsibility for this function to the credit controller.

2.4 Approval and authorization

Approval and authorisation can be a (manual) user procedure, e.g. signing a document, or an automated (programmed) control as discussed below.

In a computerised system the authorization and approval of a transaction can be carried out far more effectively and efficiently than in a manual system. The system can be programmed not to proceed if certain conditions or controls have not been satisfied. For example:

* an order clerk who wants to place a purchase order with a supplier who is not approved by the company, will be prevented from doing so because the system will not allow an order to be initiated on the system if the supplier is not on the approved supplier (creditors) masterfile. Approval is given by the fact that the supplier is on the masterfile.
* the system may be programmed to allow a salesperson to give a discount of up to 20% to a customer to secure a sale. If the salesperson tries to give a discount above 20%, the system will not allow him to proceed with generating the invoice (sale not approved)
* making a payment by electronic funds transfer will be programmed not to proceed unless, say, two specified employees each enter a unique password to effect the transaction
* the programme checks against preset parameters e.g. an online loan application is automatically approved if income and expenditure of the applicant satisfies preset parameters (only appropriate for loans of a small amount).

The point is that a computerised system is very effective at ***preventing*** unauthorized transactions from taking place. It is certainly true that these kinds of controls can be overridden, but overrides will be logged (isolation of responsibility) by the computer and should be followed up. Logging and follow up is a detective control.

The system may also be programmed to enable authorization/approval to be given on screen (on the system) by the authorizing person. This is very common in modern systems as it speeds up authorisation procedures and is very effective in preventing a transaction from progressing through the system until approval has actually been given. In a manual system (or in a computerised system where documents are printed out for approval) it is normally a case of presenting the document to the authorizing person who looks at the supporting evidence and signs the document. In a computerised system approval can be given on the system itself. How this is done may vary (depending on the software) but the principle is as follows. Employee A prepares the documents on the screen. On completion, Employee A selects the ***send*** option and his terminal transmits a message to Employee B's terminal (the authorizing employee), alerting him to the fact that the (computer) file containing the documents is ready for authorization/approval. Employee B accesses the file, carries out whatever checking procedures are necessary and if satisfied, selects the ***approve*** option on the screen. Once the approve option has been selected, the file cannot be written to at all. This prevents Employee A (or anyone else) from adding to the file after it has been approved. A refinement of on screen approval is that Employee B should not have ***write*** access to the file; any changes

should be referred back to Employee A to make the changes and re-submit the file for approval. This is good division of duties and isolates responsibility.

Consider the following example:

* Joe Bigg, the order clerk prepares a batch of purchase orders on the system which must be reviewed/approved by the chief buyer.
* Once Joe Bigg has created the file of all the purchase orders on the screen, he selects the send option and a message is sent to Chas Chetty's (the chief buyer) computer alerting him to the fact that the file of purchase orders is ready for his review and approval. From this point there will be no write access to the file
* Joe Bigg's user profile allows him to create a purchase order but not to approve it. This restriction is enforced by the system not providing an ***approve option*** on Joe's screen. The only thing that Joe can do is send the file on to Chas Chetty. Chas Chetty conducts his reviews and if he is satisfied, selects the approve option
* Because Chas Chetty has the power to approve in terms of his user profile, his screen will display an approve option, but he will not be able to change the file as he has not been granted write access. The computer will simply not respond if he attempts to alter a figure or detail on the purchase order.
* When Chas Chetty selects the approve option, the file is transferred back to Joe Bigg who can then proceed with distributing the purchase orders to suppliers by printing hard copy, faxing or e-mailing the purchase orders. As write access to the file of purchase orders is not available, Joe Bigg cannot add or change the purchase orders after they have been approved by Chas Chetty.
* If Chas Chetty requires changes to the purchase orders, e.g. he may want to reduce the quantity ordered, he will select an option which returns the file to Joe Bigg and simultaneously lifts the "no write" restriction on the file. Joe Bigg makes the corrections and repeats the procedures to get the file approved
* Until the file has been approved, the purchase orders cannot be printed or sent electronically.

In a manual system, Joe Bigg would have to write out the purchase orders in multi-copy form (lots of potential mistakes in this procedure!) and physically take them to the chief buyer who would probably sign each purchase order.

Another advantage of approval on the system is that the parties involved do not have to be geographically close. Joe Bigg could be sitting at a division of the company in Durban and Chas Chetty could be sitting at head office in Johannesburg and the approval could take place on the company's wide area network.

One potential risk with regard to approval/authorization in a computerised system is that the initiation and execution of transactions may be automatic with no visible or actual authorization of the transaction, e.g. the rate of interest paid on a savings account at a bank, or the rate of interest charged on a debtor's account by a company, may automatically increase when the savings balance reaches a specified amount or the debt has been outstanding for a specified period of time. These automatic transactions should be logged by the computer and reviewed by a suitable employee e.g. in the case of the debtors interest charge, by the credit controller.

2.5 Custody

Application controls play an important role in the custody of the company's assets particularly the company's cash in the bank and other assets held in electronic form such as the debtor's masterfile. In reality, all information on the database should be considered as an "asset" which needs to be strictly controlled as without its information, a company is in serious trouble. You can see quickly enough that if a company does not have application controls (both user and automated) in place to prevent and detect certain invalid actions, the asset is under serious threat.

* In the case of ***cash in the bank***, the company does not have physical control over the cash, but must control unauthorized removals from its bank account. In a manual

system, this will be done by controlling the company cheque book itself, limiting signing powers to senior officials (preventive controls) and reconciling the company's cash book with the bank statement (detective controls). In a computerised payment system, e.g. EFT for the payment of creditors and employees, far stricter application controls must be implemented over access to the EFT facility (the equivalent of the cheque book) and authorizing and releasing the funds (the equivalent of signing a cheque). Reconciliation of the company records and bank statement will still be an important control but can be done much more timeously as bank statements can be instantly downloaded from the bank shortly after the EFT payments have been made, and any problems can be followed up immediately. Failure to adequately protect an "on line" bank account would probably have greater consequences than losing a cheque book or having a cheque signature forged (a cheque can be "stopped" but an EFT can't), so controls to prevent invalid EFTs must be comprehensive. There will also be detective controls, but these may be "too little too late" as the money will be long gone.

* In the case of ***protecting debtors*** it is a matter of protecting the ***information*** about the debtor held in the masterfile, transactions files and supporting documentation. If the electronic information is corrupted or destroyed, the company is going to find it very difficult to reconstruct its records. In addition, if a debtor is not sent an up to date statement or request to pay (difficult to do if the company don't have records), a percentage of debtors won't pay.

In a manual system, protection will come down to keeping the accounting records under lock and key when they are not in use, and filing at least two copies of the sales invoices securely and in different places.

In a computerised system, the electronic data are protected by a combination of general and application controls. Whilst hardcopy documentation e.g. sales invoices, etc, can be physically protected, electronic files will be protected by a whole range of controls, including controlling unauthorised access of the system at systems level and application level (preventing unauthorized people from getting onto the system and if they are authorized to be on the system, from gaining access to the debtors application), as well as adequate continuity of operations controls. These will include physical controls to protect the system as a whole, as well as disaster recovery controls.

Modern software will also have features which protect the debtors information. For example, current software will not permit a person who has access to the debtors masterfile to simply delete a debtor without trace. The debtors balance would first have to be reduced to nil by valid means, e.g. processing a payment from the debtor or processing a credit note. Removal of the debtors record could then take place but this privilege would be restricted to a minimum number of employees and the removal would be logged. The most important application controls however, will probably be those which are implemented over masterfile amendments (see pt 4) in the first place.

Don't forget that these principles and controls will apply to all the company's financial information, electronic and physical.

2.6 Access controls

Once a person or terminal is introduced into a system, suitable access controls must be implemented for that terminal and employee. Access violations can have extremely serious consequences for the business. These include

- destruction of data
- "theft" of data
- improper changes to data
- recording of unauthorized or non-existent transactions

* Access to particular applications can be restricted to particular terminals, e.g. the ability to affect an EFT transfer can be restricted to the terminal of the financial manager . Note:

while modern software concentrates on restricting access through personal user profiles, access can also be limited to certain terminals.

* Access is restricted in terms of user profiles/access tables at both systems level and applications level, for example:
  - at systems level, access to a particular application may be restricted to particular users,
  - at application level, access to specific programme functions may be restricted to particular users on the "least privilege" basis e.g. sales order entry is limited to telesales operator.
* PC time out facilities and automatic shutdown in the face of access violation will prevent continued attempts to access the system, as well as the threat of employees leaving their terminals unattended.

Note (a): Physical access to computer facilities in general and access controls at system level are covered under general controls. The above access controls deal with controls at the application level.

Note (b): Once a user or PC has been granted access to a particular application, the "least privilege" principle may be implemented in a number of ways to restrict such access to the minimum possible privileges necessary for proper performance of the duties concerned:
  - restrictions on access to a module or programme function e.g. masterfile amendments,
  - restrictions in terms of mode (type) of access e.g. read-only,
  - restrictions in terms of time of day (e.g. working hours only as in a bank or telesales call centre – assists in ensuring access is supervised),
  - extent of access to data (e.g. allowing only restricted views of certain data so that sensitive data fields are hidden to users of lower privilege levels).

Note (c): Access at application level should be logged so that details of the activity carried out are recorded together with the user ID responsible for that activity (such logs can be selectively set so that only specific types of activity which have been identified as high risk are monitored).

Summary: in effect a user
* must ***identify*** himself to the system with a valid user ID
* must ***authenticate*** himself to the system with a valid password
* will only be given access to those programmes and data files to which he is ***authorised*** to have access in terms of his user profile.

Once the user has got onto the system, access is usually controlled by what appears or does not appear on the user's screen. For example, only modules of the application to which the user has access will appear on the screen, or alternatively all the modules will be listed but the ones the user has access to, will be highlighted in some way, e.g. a different colour. If the user selects (clicks on) a module to which he does not have access (this is determined by his user profile), nothing will happen and/or a message will appear on the screen which will say something like ″access denied″. In another similar method of controlling access, the screen will not give the user the option to carry out a particular action. For example, certain sales orders awaiting approval from the credit controller, are listed on a suspense file. Although other users may have access to this file for information purposes, when they access the file, their screens will not show an approve option, or the approve option will be shaded and will not react if the user clicks on it. Only the credit controller's screen will have an approve option which can be activated.

2.7 Comparisons and reconciliation

A reconciliation is a comparison of two different sets of recorded information or of recorded information and a physical asset. In a manual system this is done by employees laboriously comparing the two sets of information to identify differences. For example, an employee reconciles the net wages paid in wage period 2 to the net wages paid in wage period 1 to establish if, and why they are different. This can take a long time as changes in the number of

employees, pay rates, and deductions could all contribute to the difference. In a computerised system this reconciliation can be completed accurately, comprehensively and in no time at all. Before authorizing the payment of wages, the paymaster or accountant could review the reconciliation and tie it up to other sources of information. For example, an amount in the reconciliation which relates to changes in pay rates could be checked against the original authority for the change.

Along with the ability for a good computerised system to produce any number of reports, including those which can be printed out and used for physical comparisons, its ability to instantly compare any data on the system makes comparison and reconciliation a valuable and effective control activity.

2.8 Performance reviews

These control activities include, inter alia, reviews and analysis of actual performance versus budgets, forecasts and prior period performance as well as relating different sets of data to one another. In principle, performance reviews in manual systems and a computerised system do not differ. The huge advantage which a computerised system has is its ability to produce numerous useful reports, including comparisons, reconciliations and reasons for differences. For example, provided the necessary data is in the database, sales can be extensively analysed, reports can be generated to show what quantities of products are selling, which specific models or colours or sizes are most popular or are not selling, what gross profit is being generated from each sale, the region in which the products were sold, etc. Debtors can be analysed in terms of what they buy, how much they spend, who returns goods for credit, why credit notes were issued, how long the debt has been outstanding, etc.

In modern systems, transactions can be tracked on screen through the system as they are carried out. For example, orders from customers will start out listed on a sales order suspense file. When the time comes for the goods ordered to be picked, the sales order will be "coded/ moved" to a picking slip suspense file, and once the goods have been picked (physically) the picking slip is "coded/moved" to the invoice file. All these files are on the system, which means that at any time a manager can access the files and establish the stage the original sales order has reached. This can be done remotely, so a manager in Port Elizabeth can find out and review the performance of dispatch staff at the warehouse in Johannesburg.

3. CONTROL TECHNIQUES AND APPLICATION CONTROLS

This section of the chapter is reasonably long and detailed, so the following index has been provided to help you find your way around the section.

3.1 Batching
- 3.1.1 batch entry, batch processing/update
- 3.1.2 on-line entry, batch processing/update
- 3.1.3 on-line entry, real time processing/input

3.2 Screen aids and related features

3.3 Programme controls – input and processing
- 3.3.1 programme checks – input
- 3.3.2 programme checks – processing

3.4 Output controls

3.5 Logs and reports

4. Masterfile amendments (masterfile maintenance)

3.1 Batching

Batching is a technique which assists in controlling an activity which will be carried out on a batch of transactions with the intention of making sure that all transactions in the batch were subjected to the activity and the activity was carried out accurately and that no invalid transactions were added to the batch. Batching can be manual (user) or automated or a combination of both.

In the context of accounting systems, batching can be used at the input stage, processing stage or output stage. However modern accounting software is designed around real time input and processing in terms of which individual transactions are captured and processed almost instantaneously (real time). As up to date information is required it is no longer a case of accumulating the day's sales invoices, entering them onto the system at 4pm where they are stored on the system, and then processing them over the weekend. If the company does this the debtors masterfile, the inventory masterfile and other related information will be out of date by a week and not much use to users of that information. For example, checking an order from a customer against the customer's credit limit cannot be done effectively because that customer's balance owing may be understated because credit sales made to him during the week, are not reflected.

However, batching does still have a place, for example in a wage system, where up to date information is only needed at say, two weekly intervals. The daily hours worked by each employee will be accumulated and then entered individually as items in a batch and processed in a batch. The batch could be designed as a convenient numerical number or by some other means, e.g. employees in a cost centre. Batches are processed in order. The following description of batching illustrates the principle of batching at the input stage.

* Source documents are grouped into separate batches of say 50, and the following ***control totals*** manually computed:
  - ***financial totals***: totals of any fields holding monetary amounts
  - ***hash totals***: totals of any numeric fields e.g. invoice number (meaningless other than as a control total)
  - ***record counts***: totals of the number of records (documents) in the batch e.g. 50.

* A batch control sheet should be prepared and attached to each batch. The batch control sheet should contain:
  - a unique batch number e.g. batch 3 of 6, week ending 31/7/01
  - control totals for the batch
  - identification of transaction type e.g. invoices
  - spaces for signatures of all people who deal with the batch, e.g. prepared by: ..., checked by …, reviewed by ….

* A batch register should be used to record physical movement of batches; the register should be signed by the recipient of the batch after checking what is being signed for, e.g. transfer batches of clockcards to the payroll department.

* The batch control system works as follows:
  - the details of the batch (e.g. batch description and control totals) are keyed into the computer to create a batch header label,
  - information off each record in the batch is keyed in and subjected to relevant automated validation checks e.g. valid account number, limit check.
  - when all records have been entered, the computer calculates its own control totals based on what has been keyed in and compares these totals to the manually computed totals inputted earlier to create the header label (off the batch control sheet).
  - if the totals agree and no other type of error was detected, the batch is accepted for processing, otherwise the batch is rejected and sent for correction.
  - once the control totals have been "attached" to a batch, they can follow the batch throughout the process e.g. if there are 50 clock cards in a batch, the computer will record whether 50 were ***keyed in***, 50 were ***processed*** and ***output*** for 50 was created.

Note (a): Batching assists with the following
- identifying data transcription errors (e.g. incorrect values keyed in due to transposition errors),
- detection of data captured into incorrect field locations,
- detection of invalid (e.g. duplicate) or omitted transactions or records for a batch, e.g. if a clock card is entered (keyed in) twice, the control totals will not balance.

The following summary should clarify batching in the context of transactions flowing through the system. Remember that the control hinges around creating totals "before", and "after" and then comparing these to each other.

3.1.1 Batch entry, batch processing/update

* Transaction data is captured initially onto manually prepared source documents e.g. sales invoices.
* These source documents are then collected into batches usually after manual checks have been performed and entered via the keyboard with control totals in these batches. Relevant programme checks take place as the information is keyed in. The transaction information is converted into machine readable form and held on a transactions file on the computer system.
* These transactions are then processed as a batch when it is efficient/convenient to do so and the relevant masterfiles are updated to reflect the effect of the entire batch on affected masterfile balances. Control totals before and after processing are compared.
* Not common, particularly as it is slow and information is not up to date.

3.1.2 On-line entry, batch processing/update (also referred to as on line entry with delayed processing)

* Transaction data is entered, via a keyboard immediately as each transaction occurs. e.g. a sales order is placed by telephone and the operator keys in the details as the conversation with the customer takes place. Relevant programme checks take place as information is keyed in (for simplicity sake, assume an invoice is created immediately and not only after goods have been dispatched).
* The transaction information is converted into machine readable form as each transaction occurs and is held on a transactions file on the computer system.
* Control totals are created by the computer on the batch for the transaction file.
* The transactions are then processed as a batch and the relevant masterfiles are updated to reflect the effect of each transaction in the batch on affected masterfile balances, e.g. they could be processed at the end of each day (daily batch update).
* Entry of the transaction is efficient, but information is not immediately up to date. The longer the period that the batch of transactions is not processed, the less up to date the information.

3.1.3 On-line entry, real-time processing/update

* Transaction data is entered via a keyboard, immediately as each transaction occurs. Relevant programme checks take place as information is keyed in.
* The relevant masterfiles are also updated immediately to reflect the effect of each individual transaction on affected masterfile balances, e.g. a seat booked on an aircraft will instantly update the "seats available masterfile" which is really an inventory masterfile for that particular flight. Obviously this could not be done in batch mode as the same seat could be booked numerous times before the masterfile is updated.
* Entry of the transaction is efficient (access controls are very important) and information is right up to date.

3.2 Screen aids and related features

Screen aids have been classified as all the features, procedures or controls which are built into the application software and reflected on the screen to assist a user to capture information accurately and completely, and to link the user's access privileges to the screen in front of him.

For example, if an employee does not have the power (privilege) to approve an onscreen document, there may be no "approve" option for the document appearing on the screen. The employee may only have a send option. Alternatively the "approve" option may be on the screen but may be shaded and will simply not react if the user "clicks" on it.

* ***minimum keying in of information***. The principle is that the less information that has to be keyed in, the less errors are likely to occur and the less time it takes, e.g.

- in a telesales system, the customer should be required to give only his account number or name which, when keyed in, will automatically retrieve all other standing details, provided the account number is valid. It thus makes it unnecessary for the person taking the order to key in name, delivery address etc.
- techniques such as "drop down" lists which simply require the user to "select and click" the option they require from the options provided on the dropdown list.

* The screen should be formatted in terms of what hardcopy would look like e.g. when entering an order from a customer the screen should look like the sales order, and should have easily recognisable fields into which data is entered such as a box with the letters QTY (quantity) above it. Another example is that where possible, the number of little boxes within a field box should reflect the number of digits required for that field, e.g. a person's identity number has thirteen digits, so the identity field should consist of thirteen little boxes. The ***screen should be formatted*** to receive essential data in the order in which it is required, e.g. the debtors account number is at the top.

* extensive use of ***screen dialogue and prompts***. These are messages sent to the user to guide him, e.g. a prompt may appear on the screen reminding the user to confirm and re-enter a field.

* ***mandatory fields.*** Keying in will not continue until a particular field or all fields have been entered. Such fields may be hi-lighted in red or identified by a star or there may even be a prompt if the user misses out that field and moves on to the next field.

* ***shading of fields*** which will not react if "clicked on", e.g. an on-screen sales order may have the customer's account number and details shaded, the user completing the sales order will not be able to change these fields.

3.3 Programme controls - input and processing

Programme checks are controls which are built into the application software, with the intention of validating/editing information/data which is entered or processed. Validation can take place at the input and/or processing stages. Vast quantities of transactions can be subjected to a range of programmed controls to consistently produce reliable information. Errors are reduced and information is provided timeously ***but*** remember that a computer does what it is programmed to do, so although input controls may be very good, an error in (processing) programming can undo these benefits and the error will be processed over and over again. Programme checks are many and varied. The list below provides a number of common programme checks, sufficient to illustrate the kinds of controls which can be implemented. The list is not exhaustive. Some checks are very similar to others and the same check is often given a different name by software providers and users. Not all programme checks are relevant to all applications by any means. As an auditor, you need a general understanding of what the programme check does, regardless of its name, so that you can recognise the different checks when you are working at different clients. Also remember that programme checks do slow things down and take up computer resources.

3.3.1 Programme checks - input

* ***Existence/validity checks***

- ***validation checks*** validate data keyed in against the masterfile e.g. a customer's account number will be checked against the debtors masterfile.
- ***matching checks*** are described in different ways, but essentially they amount to input being matched against data that is already in the database. Checking input information against data on a masterfile is a form of matching, as is matching a biometric characteristic of an employee (thumbprint) against the employee masterfile. The computer may also match the details of an invoice received from a supplier to the corresponding GRN held in a suspense file on the system.
- ***data approval/authorisation checks*** test input against a preset condition e.g. to make a sale on credit, a liquor store requires that a customer's identity number be entered on a computer generated invoice. If the customer is under 18 (which the identity number will indicate), a

sales invoice cannot be generated. (The sale is not authorised). Another example would be where the credit limit on a debtors account can only be 30 or 60 days. An attempt to enter 120 days in the credit terms field would not be approved.

* ***Reasonableness and limit checks***

- ***limit checks*** detect when a field entered does not satisfy a limit which has been set, e.g. the normal hours worked by an employee in a week cannot be entered at a quantity greater than 40 hours.
- ***reasonableness checks*** for the data being entered to be accepted, it must fall within reasonable limits when compared to other data, e.g. if a normal order from a customer for an inventory item is 100 units, and a clerk enters 1000, the screen will display a message querying the entry of 1000, although there is no limit on the quantity ordered. (The computer does an "instant" check on the quantity that the client normally orders). Of course this type of check takes processing resources, so will only be used if there is a real benefit.

* ***Dependency checks***

An entry in a field will only be accepted depending on what has been entered in another field, e.g. the acceptability of entering a credit limit of R100 000 on a debtors account will depend on the status allocated to the debtor. If the debtor's credit status rating is A+ (very good) the credit limit of R100 000 will be acceptable. If the status is only B+ then the credit limit will not be acceptable.

* ***Format checks***

- ***alpha-numeric checks*** prevent/detect numeric fields which have been entered as alphabetics and vice versa, e.g. when entering an employee's identity number, all digits must be numeric.
- ***size checks*** detect when the field does not conform to pre-set size limits, e.g. an identity number entered must have 13 digits.
- ***mandatory field/missing data checks*** detect blanks where none should exist, if a quantity is not entered in a quantity field on an internal sales order, data capture cannot continue. (This is also discussed under screen aids.)
- ***valid character and sign check.*** The letters, digits or signs entered in a field are checked against valid characters or signs for that field, e.g. a minus sign (-) could not be entered in a quantity order field.

* ***Check digits.*** A check digit is a redundant (extra) character added to an account number, part number etc. The character is generated by manipulating the other numerical characters in the account number. When the account number is keyed in, the computer performs the same manipulation on the numerical characters in the account number and if it has been entered (keyed in) correctly, the computer will come up with the same check digit which was added to the account number originally. If it does not match, the computer sends a screen message to inform the operator that the account number has been incorrectly entered. Check digits use up processing resources and therefore are limited to critical fields. They ***cannot*** be used on financial fields.

* ***Sequence checks*** detect gaps or duplications in a sequence of numbers as they are entered, e.g. if numbered masterfile amendment forms are being keyed in, a sequence check will alert the user if there is a gap or duplication in the numerical series.

Note: The controls which follow are not programme controls, but where information is entered off a source document the source document should be

- pre-printed, in a format which leaves the minimum amount of information to be manually filled in
- pre-numbered; sequencing facilitates identification of any missing documents
- designed in a manner which is logical and simple to complete and subsequently enter into the computer, e.g. key pieces of information should have a prominent position on the document
- should be designed to contain blank blocks or grids which can be used for authorising or approving the document.

Unused source documents should be kept under lock and key by an independent person and a register of receipt and issue of the document kept. If the source document is freely available, it is easier to create fraudulent transactions.

3.3.2 Programme checks – Processing

Processing controls assist in ensuring that data is processed accurately and completely. Processing is a combination of elements in the system, e.g. masterfiles, transaction information which has been input, programmes and the hardware itself. All elements must be controlled if only authorised transactions which have actually occurred, are to be processed accurately and completely. Obviously the user cannot "see" processing taking place, but the computer will be programmed to carry out checks on itself and "report" to the user on what it has done. The user can then satisfy himself that processing occurred accurately and completely.

Processing will not normally stop if an error is discovered. The error will be written to an exception report.

* *Programme edit checks*

Some examples of edit checks which the computer may carry out are as follows:

- ***sequence test.*** The sequence of documents processed is checked for gaps, e.g. after processing credit notes, the computer may identify missing credit note numbers.
- ***arithmetic accuracy check*** e.g. reverse multiplication, (multiplication is repeated but in reverse and answers matched 3x6 = 18; 18÷6 = 3).
- ***reasonableness/consistency/range tests.*** After processing of a transaction has taken place, the result is compared by the computer itself to other information for reasonableness e.g. a wage of R5000 is not reasonable for a grade 3 employee or compared to his prior wage period's earnings.
- ***limit test*** identifies amounts which fall outside a predetermined limit after processing, e.g. credit sales to a customer have pushed the debtor's balance owing beyond the customer's credit limit.
- ***accuracy test***. Where amounts are allocated to columns and the columns are independently cast (added up), the totals of the columns can be cross cast (added across) and compared to the total amount allocated e.g. net pay + paye + medical aid deduction = gross pay.
- ***matching*** in the context of processing is about comparing data which has been processed, against data which is already in the database, e.g. a matching control may match clock cards processed with the employee masterfile to identify employees for whom there was no clock card information. The reason there is no clock card may be perfectly valid, e.g. the employee was on holiday for the week, but it could also be a processing error.

* *Programme reconciliation checks*

The computer will also carry out reconciliations of control and other totals in one form or another, based on the principle that if pre-processing totals and post-processing totals can be reconciled, we can be more confident that processing was valid, accurate and complete.

- ***control totals***, e.g. record counts, hash totals from input are compared to record count and hash totals after processing.
- ***run-to-run totals***. A final balance arrived at after processing is compared to the opening balance and individual totals of transactions e.g. the closing balance on debtors (31 May) is compared to the opening balance on debtors (30 April) plus the total of May sales (debits) less the total of May receipts (credits).

Note: Reliable and correct processing would be affected if the wrong data files and programme files were used for processing. This occurrence should be prevented by the library software and database management system and is well beyond the scope of this text.

Note: The reliability of the hardware itself, will also play an important part in processing. Modern computer equipment is very reliable, and the hardware will have its own range of hardware controls, e.g.

- ***parity checks***. A redundant bit is added to data to make the sum of the bits in the data concerned, even (even parity) or odd (odd parity). Changes in parity detected as a result of this check indicate that an error has occurred in transmission or processing.

- ***valid operation code.*** The processor checks if the instruction it is executing is one of a valid set of instructions.
- ***echo check.*** The processor sends an activation signal to an input/output device – that device returns a signal showing it was activated. Echo checks can also be used to detect corruption of messages in transit by bouncing the signal back from the recipient of the message to the sender so that the sender can compare it against the original message for any errors, which may have occurred during transmission.
- ***equipment check.*** Input/output devices are activated prior to a read/write operation to ensure they work correctly.

Evaluating hardware is the domain of the expert not the general auditor, and will be considered when conducting risk assessment procedures.

Note: Interruptions in processing which could lead to errors in processing, will be logged on activity reports and will be followed up by operations staff.

3.4 Output controls

The objective of output controls is to ensure that output (which is the product of processing) is accurate and complete and that its distribution is strictly controlled, for example, confidential output does not go to the wrong individuals. Output does not have to be in hardcopy, it can be "on screen". The accuracy and completeness output controls will be strongly aligned with processing controls, because, if processing has proved to be accurate and complete, the data which is turned into reports for users is far more likely to be accurate and complete.

* ***controls over distribution will include preventive controls such as***

- clear report identification
  - name of report
  - time and production number of report (this prevents confusion if the report is run more than once)
  - processing period covered (assists in carrying out checks against input data)
  - sequenced pages and "end of report" messages (prevents undetected removal of pages)
- a distribution matrix of who is to receive which output and when. This should align with the user profiles and access privileges of employees so that individuals who do not need access to the reports etc, cannot access them on the system
- if output is hardcopy and printed out at a certain point and distributed to users, its movement should be controlled by the distribution list (who gets what and when), and an entry in a register which is signed by the authorized recipient on receipt of the output
- output which is confidential should be designed to promote confidentiality, e.g. "sealed envelope" salary slips
- confidential information for employees which is emailed to them (such as payslips again) should ***not*** be emailed to their work PCs
- output which is printed out, especially more sensitive information, should be printed out only in the departments which require the output, and if it is confidential, under the supervision of authorized personnel
- output which is not required should be shredded, not just left about or thrown away as a complete document.

* ***user controls will include (all detective controls)***

- review of output for completeness e.g. numerical sequence check
- reconciliation of input to output e.g. foreman of each cost centre reconciles overtime worked with his factory overtime records
- review of output for reasonableness e.g. financial manager reviews period-to-period wage reconciliations (payroll manager will conduct detailed tests on the period-to-period wage reconciliation produced by the system)
- review and follow up of any exception reports produced during processing e.g. individual wage payments which failed "reasonableness test" during processing.

3.5 Logs and reports

Logs and reports do not have to be printed (but often are). They can be accessed on screen. Access can be restricted to read only and should be for all logs of computer activity which form part of the audit trail.

The types of logs and reports that may be produced by a computer are virtually unlimited. These may be used as detective or monitoring controls to provide additional assurance that computer processing is valid, accurate and complete and that computer usage is authorised and productive. It is important to be selective about use of logs and reports as they can affect computer performance (slower processing and use of storage space). They also require review and follow up, so unless personnel are allocated to do so, the logs and reports themselves are worthless. Types of logs and reports used may include:

* ***audit trails***, provide listings of transactions and summaries and lists of tables or factors used in processing.

* ***run-to-run balancing reports***, which provide evidence that the opening balances which have been updated by a series of transactions have resulted in correctly calculated closing balances.

* ***override reports***, which provide a record of computer controls which have been overridden by employees using supervisory or management privileges. Abuse of such privileges is a threat to the objective of validity.

* ***exception reports***, which provide a summary listing of any activities, conditions or transactions which fall outside of parameters which have been set for control purposes, e.g. employees whose remuneration for the wage period falls outside the reasonableness parameters set for employees of that grade.

* ***activity reports***, which provide a record for a particular resource, of all activity concerning that resource e.g. names of users, usage times and duration of usage.

* ***access/access violation reports,*** particularly important in relation to sensitive applications such as electronic funds transfer and payroll.

These are categories of reports, hundreds of different reports falling into these categories may be produced in a reasonably sized business.

4. MASTERFILE AMENDMENTS (MASTERFILE MAINTENANCE)

In a computerised financial accounting system, the masterfile contains very important data which, if not protected from ***unauthorized*** change, can have very negative results for the company. For example, unauthorized increases to employees' pay rates in the employee masterfile, or to debtors' credit limits in the debtors masterfile or the addition of an unapproved supplier to the creditors masterfile could all result in losses to the company at a later stage. If the quantity field in the inventory masterfile is not protected from unauthorized amendment, a theft of inventory could be covered up by reducing the quantity field in the inventory masterfile. Therefore the application controls over masterfile amendments are very important. The objective will be that

* only valid (authorized) amendments are made to masterfiles
* the details of the amendment are captured and processed accurately and completely
* all masterfile amendments are captured and processed.

The controls are based on the principles discussed in this chapter and will be a combination of a user and programme controls and will include both preventive and detective controls (and correction controls when applicable). As usual, the focus will be on preventive controls.

An example of the controls over a debtors masterfile amendments is given on the next page.

Procedure	*Application controls and related comments*
1. Record all masterfile amendments on a source document.	1.1 ***All*** amendments to be recorded on hardcopy masterfile amendment forms MAFs (no verbal instructions). 1.2 MAFs to be pre-printed, sequenced and designed in terms of sound document design principles.
2. Authorise MAF.	2.1 The MAFs should be • signed by two reasonably senior debtors section personnel e.g. credit controller and senior assistant after they have agreed the details of the amendment to the supporting documentation, e.g. the approved credit application document for the addition of a new customer • cross referenced to the supporting documentation.
3. Enter only authorized masterfile amendments onto the system accurately and completely. .	3.1 Restrict write access to a specific member of the debtors section by the use of user ID and passwords. 3.2 All masterfile amendments should be automatically logged by the computer on ***sequenced*** logs and there should be ***no write access*** to the logs (this allows subsequent checking of the MAFs entered for authority) 3.3 To enhance the accuracy and completeness of the keying in of masterfile amendments and to ***detect invalid conditions***, screen aids and programme checks will be implemented ***screen aids and related features*** * minimum keying in of information. For example when amending existing debtor records, the user will only key in the debtors account number to bring up all the details of the debtor * screen formatting, screen looks like MAF, screen dialogue * new debtors account number automatically generated by the system ***programme checks*** e.g. * verification/matching checks to validate a debtor account number against the debtors masterfile (invalid account number, no amendment) * alpha numeric checks * range and/or limit/data approval checks on terms and credit limit field, e.g. credit limit must be between R5 000 and R75 000 (range) or cannot exceed R75 000 (limit), and terms can only be 30 days or 60 days (data approval) * field size check and mandatory/missing data checks, e.g. credit limit and terms must be entered when adding a new debtor * sequence check on MAFs entered * dependency check e.g. the credit limit granted may depend upon the credit terms granted, e.g. a debtor granted payment terms of 90 days may only be granted credit up to a limit of R2 000 (a relatively low amount)
4. Review masterfile amendments to ensure they occurred, were authorized and were accurately and completely processed.	4.1 The logs should be reviewed regularly by a senior staff member e.g. financial manager 6.1 the sequence of the logs themselves should be checked (for any missing logs) 4.2 Each logged amendment should be checked to confirm that it is supported by a properly authorised MAF and 4.3 That the detail, e.g. debtor account number, amounts, etc, are correct 4.4 The MAFs themselves should be sequence checked against the log to confirm that all MAFs were entered.

Note (a): Modern accounting packages do not allow ***balances*** in a masterfile to be adjusted other than through a sub-routine (sub journal), e.g. it is not usually possible to go into the masterfile via the masterfile amendment module and reduce or delete a debtor's balance. This would have to be done through a transaction file, e.g. credit notes, journal entries or receipts.

Note (b): Unused MAFs and other important supporting documentation should be subject to stationery controls as it is more difficult to create an invalid masterfile amendment without the source document.

Note (c): A masterfile amendment should be carefully checked in all respects before it is authorised, e.g. the validity of credit terms and limits to be entered, so there should not be too many errors or invalid conditions having to be identified by the programme controls. Each company will decide for itself the extent of programme controls they wish to implement.

COMPUTER ASSISTED AUDIT TECHNIQUES (CAATs)

1. INTRODUCTION

Computer assisted audit techniques are exactly what they sound like: making use of a computer to assist in carrying out the audit. Although there is some extremely powerful and complex software available to assist in performing audits, the concept is simple: wherever it is economical and efficient to do so, the power, speed and versatility of the computer should be harnessed to assist with the audit. For many audit clients, it would simply be impossible to perform an audit without using CAATs. Consider a very simple example;

A branch of a major bank has 22 371 account holders who have call account deposits with the bank, which earn interest on daily balances. At the year end audit, we need to confirm that total interest paid on these call accounts (as well as various other savings accounts, fixed deposits etc.) has been correctly calculated, as reflected in the financial statements at R71 587 200.

* imagine trying to obtain printouts of all 22 371 account holders and each of their daily balances for 365 days and then trying to test enough of these on our calculator, to form a representative sample of interest calculations – clearly impractical, tedious, inefficient, very expensive and a high probability that our audit staff would make many mistakes themselves along the way!
* Instead we are able to use audit software, which can reperform all of these daily balance calculations and provide an independently calculated total for interest payable by the bank for the year. Powerful CAATs packages are able to do 100% testing like this incredibly quickly thus providing huge benefits to auditors by significantly reducing audit risk (100% testing rather than sample testing), providing more reliable evidence (no human errors) and increasing audit efficiencies (millions of calculations can be reperformed in a matter of minutes and hours rather than days and months.)

2. HOW DO CAATs FIT INTO THE AUDIT PROCESS?

The auditor decides whether or not to use CAATs when considering the audit strategy (***scope, timing*** and ***direction***) and the audit plan, (***nature, timing*** and ***extent*** of testing) which is necessary to reduce audit risk to an acceptable level (refer to Chapter 6 to refresh your memory if necessary). The decision made will result in the auditor taking one or more of the following approaches:

* to audit around the computer,
* to audit through the computer,
* to audit with the computer.

The auditor is not restricted to selecting just one of these approaches. For further discussion on this see para 2.4 below.

2.1 Auditing around the computer

* This approach treats the computer system and programmes as a black box and relies on review and comparison of the input and output documents. The rationale behind this approach is that if the source documents are valid, accurate and complete, and the output produced by the computer system as a result of processing these source documents, is correct, then the processing functions of the computer system are being performed correctly. The manner in which these processing functions are performed is deemed to be of little consequence. This approach assumes that the ***computer generated output can be traced back, and compared to the input***.

* The audit is performed by selecting a sample of transactions that have already been processed and then tracing these transactions from their point of origin as source documents to the output documents or records produced by the computer system.

* This approach is only feasible if the computer system under consideration is a simple, batch oriented system with ***no significant controls or automated/integrated functions built into the system***.

* Additional requirements for the adoption of this approach are that control is maintained by segregation of duties, independent checks and management supervision together with the ***maintenance of a clear audit trail.***

* The main ***advantages*** of auditing around the computer may be summarised as follows:

  - there is no risk of corruption of the client's data by the auditor,
  - the auditor requires little or no knowledge of computer technology,
  - there is minimal disruption of the client's IT function,
  - the costs associated with technology and computer expertise may be reduced.

* The ***disadvantages*** of auditing around the computer may be summarised as follows:

  - apart from the more trivial applications, computer systems generally involve volumes of data and transactions which render manual testing ineffective,
  - system controls and potential errors within the system are ignored,
  - no use is made of the most powerful and valuable audit tool, namely, the computer.

2.2 Auditing through the computer

* This approach is concerned with testing the computer system and controls which are built into the system.

  - Simplistically this is achieved by the auditor sending transactions (test data), some of which will contain errors which the system's programme controls should detect, through the system. In this way the auditor tests whether controls are working as expected e.g. if a transaction which the auditor knows is incorrect ***is*** picked up by the system, the auditor has some evidence that the system is working (and vice versa). Thus auditing through the computer is primarily a "test of controls" approach.

* The main ***advantage*** of "auditing through the computer" is that it can be used effectively and efficiently to audit a highly sophisticated computer system which processes huge volumes of data and relies extensively on computerised controls, e.g. banks.

* The ***disadvantages*** of "auditing through the computer" include:
  - the auditor is required to have a high level of technical computer knowledge,
  - audit costs may increase due to the level of investment in technology and expertise required,
  - the auditor is required to take stricter precautions due to the increased risk of corruption of the client's data and masterfiles.

- a high level of client co-operation is necessary which may impinge upon audit independence.

2.3 Auditing with the computer

There are two aspects to "auditing with the computer":

- using the computer to assist in the performance of audit procedures (mainly substantive testing).
- using the computer to produce electronic/automated workpapers, audit programmes and financial statements.

Using this approach for substantive testing, involves gaining access to a client's files and using audit software (programmes which help the auditor to do what he has to do) to read, sort, compare and analyse data on the file, very quickly and extensively.

The idea behind using the computer to automate the audit is to make it a more effective and efficient audit by harnessing the power of the computer.

* The main ***advantage*** of auditing with the computer is that use is made of the power, speed and versatility of the computer which results in a more economical and efficient audit.

The ***disadvantages*** are:

- costs/licence fees of audit hardware and software
- the audit team requires training on how to use the software
- there ***may*** be a tendency for the audit team to audit without thinking about what they are doing.

2.4 Combinations of the above approaches

As indicated in the introduction to CAATs, the auditor is in no way restricted to one of the three approaches. In probably 99% of reasonably sized audits, where the client has a computerised accounting system, the audit approach will be a mixture of the above approaches. Auditing is about getting the mix of tests of controls and substantive testing right, based on the strength of the organisation's controls and the ease/efficiency with which substantive testing may be achieved. Also remember that some of the procedures which the auditor carries out, may be unaffected by whether the client is computerised or not e.g., scrutiny of minutes, or inspection of non-current assets. The overriding objective is to achieve the most effective and efficient way of getting the audit done.

3. SYSTEM ORIENTATED CAATs

As suggested by their description, these CAATs concentrate on the accounting system and related control procedures and are used predominantly to perform tests of controls, although some substantive evidence may also be produced. The use of systems orientated CAATs is regarded as "auditing through the computer."

3.1 Test data

This type of CAAT requires the auditor to ***create*** a set of transactions (let's assume clockcards) to be keyed in and processed. The transactions will include both correct data and incorrect data; i.e. a clockcard with an invalid employee number and another with 55 hours of normal time, will be entered. What the auditor expects is that the invalid employee number will be identified by the computer and written to an error report, and that the 55 hours normal time will be identified by the programmed input limit check and the error highlighted immediately for correction. Obviously, if entry and processing goes ahead as normal, the controls are not working!

* Using the test data, the auditor can design transactions to test any controls which the client claims are in the system, but designing suitable transactions which contain the error conditions which the auditor wants to be prevented or detected, can be time consuming.

* For the "test data" approach to be effective, the auditor must be fully aware of the controls which are in the system and must know what the theoretical output should be so that he can compare it to the actual output for the transactions he has processed.
* As with manual tests of controls, the test data approach only tells the auditor that the control was working ***when tested*** and not that it worked throughout the whole period under audit.
* The auditor will also need to confirm that the programme tested is the one that is used in live runs.
* The test data should be run against a "copy" of the live (production) programme to prevent corruption of the client's data.

3.2 Integrated test facility (ITF)

This is really an extension of the "test data" approach. In this method, an artificial (dummy) unit is created on the client's system e.g. Company "X" or Cost Centre "Y". The auditor can then feed test transactions through the system for processing along with normal transactions. The test transactions will, however, all be coded for processing to the fictitious Company "X", which is simply excluded for purposes of the client's normal accounting purposes. This type of CAAT therefore reduces the risk of corrupting the client's information. For example, the auditor could enter two fictitious (dummy) employees on the employee masterfile, in the proper manner, e.g. employee number, cost centre, grade, payrate. He would then create fictitious clockcards with error conditions for the dummy employees and would have them processed at the same time and in the same manner as the client's genuine clockcards when the "live" payroll run is being performed. As long as they are coded to a fictitious cost centre (e.g. Cost Centre "Y"), they can easily be excluded from the client's normal financial reporting records.

* Again the auditor will need to have a clear knowledge of the controls in the system and the results which should be achieved (output).
* Once the "dummy records" have been created in the client's files, the auditor can visit the client on a number of occasions during the year under audit to perform the test; this helps to gather evidence that the controls were working throughout the year, but
* The major disadvantage of this technique is that fictitious transactions may be muddled in with the client's data if not correctly coded or if the dummy unit is not separated out before reports are sent to users. For example, the foreman might be a little surprised and confused to see two additional employees and an extra cost centre in his factory!
* It is also conceivable that client staff could manipulate ITF facilities for fraudulent purposes.

3.3 Parallel simulation

This type of CAAT involves running the client's transaction data and masterfile information through a "trusted" system set up by the ***auditor,*** as well as through the client's normal system. The results of the two processing runs are then compared and any discrepancies are followed up. These results can provide evidence relating to controls (e.g. the auditor's system may make effective use of a limit check which identifies invalid data while the client's system may not have such a check in place), as well as evidence of a substantive nature (e.g. daily transaction totals can be compared to verify accuracy of client figures).

3.4 Embedded audit facility

For this type of CAAT to operate, the auditor arranges to have an audit module inserted into the client's application programme. The module is designed to either identify transactions which might be of particular interest to the auditor, or to reperform certain validation controls and report thereon, ***while*** the client is actually running the normal application programmes. For example, the auditor may wish to identify all payments to creditors exceeding R500 000. The audit module would identify these and write them to a file. Another example is that the audit module could be programmed to perform reasonableness tests when salaries are processed and report on any items outside of given reasonableness ranges. These embedded files would have strict access controls in place and the auditor could appear at any time to audit/follow up on recorded transactions or exceptions written to the files.

4. DATA-ORIENTATED CAATs

These CAATs are concerned mainly with ***substantive testing*** i.e. obtaining evidence to support the assertions relating to balances in the statement of financial position and totals of transactions which underly the statement of comprehensive income. Use of these CAATs can be thought of mainly as "***auditing with the computer***".

4.1 Generalised/Customised audit software

These are programmes which are used to extract/analyse/reformat data extracted from client systems, e.g. auditor may extract a report of all debtors amounts outstanding over 90 days.

Common features and facilities:

* versions are generally available for use on a wide range of hardware and systems software,
* they are generally easily programmable to access various file formats and data fields thereby enhancing the ease of use for the generalist auditor,
* they are menu driven, which adds to their user friendliness,
* special security features are generally included, such as restricting certain features of the software to special classes of users.

Where generalised software (GAS) is not available to suit the needs of a particular set of circumstances, customised audit software (CAS) may be specially developed.

4.2 System utilities and report writers

Many clients will have utilities and report writers resident on their computers. Utility programmes can be used to manipulate and analyse data and test whether programmes function correctly, things which can be very useful to auditors. Report writing programmes enable users, including the auditor to design and extract various reports, which may be particularly useful in performing substantive tests.

* ***Advantages*** :
  - the software is already loaded on the client's hardware,
  - they are relatively simple to use,
  - they perform many of the tests which GAS packages offer,
  - the cost of using these packages is generally lower than using GAS.

* ***Disadvantages*** :
  - there is a wide range of utilities and report writers so the auditor will have to assess cost versus benefit of getting to know how unfamiliar client's utilities and report writers function.
  - these forms of CAAT may not be as well documented as GAS packages are, and may not quite meet the auditor's requirements.

5. FACTORS WHICH WILL INFLUENCE THE DECISION TO USE CAATs

The use of CAATs in modern day auditing is very common but this does not mean that CAATs are always an appropriate tool for every aspect of every audit. The following factors will be taken into account in making the decision as to whether CAATs should be used:

5.1 Complexity of the client's system

Where a client's accounting systems are extensively computerised and of a high level of complexity or sophistication, the auditor cannot rely on manual audit procedures alone.

5.2 Volume of transactions/output

The size of the business will usually govern the number of transactions which flow through the accounting system. As the volume increases, so do the sizes of files which result from processing the transactions, making it impractical/impossible to perform ***manual*** extraction, sorting, analysing, summarizing of data etc, due to normal audit time constraints.

5.3 Data stored in electronic form

The client will usually store data in electronic form e.g. debtors masterfile, inventory masterfile. In such cases:

- it will not be feasible/efficient to audit the data manually, and
- normal audit trails may not exist so alternatives to normal manual procedures have to be sought, for example using CAATS.

5.4 Availability of skills in the audit team

Particular skills, sometimes of a high level, are required when using some types of CAATs (but see note (a) below).

5.5 Potential loss of independence

The use of CAATs requires the co-operation of the client and where system orientated CAATs are used, the auditor may have to rely quite heavily on client personnel to run the CAAT (see note (a) below).

5.6 The attitude of the client

Professionally run companies expect professional auditors and hence will expect their auditor to be up to date with, and capable of, using advanced audit techniques (see note (a) below).

5.7 Compatibility of the firm's hardware and software with the client's hardware and software

The audit firm's hardware and software is unlikely to suit every single client's hardware and software so will need some adaptation, e.g. additional software may be required (cost), in order to run audit programmes on client systems/files (see note (a) below.).

5.8 The utilities available at the client which can assist

Utilities are programmes which can frequently perform tasks which are useful to the auditor such as sorting/re-organising files, copying, printing parts of a file, etc. They do many things which generalised audit software does, so if the auditor has no suitable generalised audit software, he may consider using the client's utilities.

NOTE (a) : 5.1 to 5.3 above are factors in favour of the use of CAATs (and really make it obligatory to do so). 5.4 to 5.7 are factors which negatively influence decisions relating to the use of CAATs, but are often outweighed by the benefits of using CAATs e.g. better quality and more extensive evidence, resulting in more effective and efficient audits and reduced detection risk. If the audit firm does not have the necessary skills, they should acquire them, or give up the audit.

6. AUDIT FUNCTIONS WHICH CAN BE PERFORMED USING DATA ORIENTATED CAATs

* sorting and file re-organisation
* summarisation, stratification and frequency analysis
* extracting samples
* exception reporting
* file comparison e.g. current masterfile to prior year's masterfile
* analytical review e.g. extraction of ratios
* casting and recalculation
* examining records for inconsistencies, inaccuracies and missing data (and creating reports thereon).

APPENDIX 1 – ILLUSTRATION OF WHAT A DATA ORIENTATED CAAT (AUDIT SOFTWARE) CAN DO.

Below is a chart of what the inventory masterfile at 30 June 0002 of an electrical supply company might look like when printed out. Of course this is a tiny part of the file, showing only seven (7) line items or records. The actual masterfile may have five thousand line items which, if printed out would produce a 160 page printout!

Item no.	Description	Location	Category	Quantity	Unit Cost	Value	S Price	Last Sale	Last Purch
A 123	Fuse Box	WH 2	A	20	710.00	14 200.00	690.00	5/0001	3/0002
P 492	Regulator	WH 3	B	-6	42.50	-255.00	56.50	2/0002	4/0002
L671	Plugs	WH 4	A	410	8.00	3 280.00	14.00	11/0001	10/0001
G 893		WH 2	C	91	44.00	4 004.00	52.75	1/0002	2/0002
	Connector	WH 1	D	18	2.20	396.00	4.20	5/0002	7/0002
Q 456	Junction		A	3	618.00	1 854.00		7/0001	8/0001
P 769	Brushes	WH 1	B	0	34.20	34.20	36.40	4/0002	6/0002

Things that can be done with audit software.

1. Scan the entire file and produce a report of missing fields or duplicated item numbers, e.g. missing item number, description, location and selling price (see item number Q456).

2. Sort the file by category, and add up value field by category to determine whether the major portion of the inventory value is of a particular category. This will provide the auditor with a better idea of where to direct the inventory audit focus.

3. Sort the file by location, and add up value and quantity fields to assist in planning attendance at the inventory count.

4. Extract a list of items with negative quantities, values or unit costs (NB a negative x a negative equals a positive - see item number P492).

5. Extract a listing of inventory items where the quantity field is zero (0) but the date of last purchase is after the date of last sale (see item number P769).

6. Reperform the quantity x unit cost calculation and compare the result to the field to identify any differences with the client's file (see connector R2.20 x 18 = R396.00?? and P769, 0 x R34.20 = R34.20??)

7. Compare unit cost field to selling price field to identify instances where cost exceeds selling price (see item number A123).

8. Extract a list of items where date of last sale is (say) more than 9 months ago, but date of last purchase is, less than 3 months ago, and by enquiry establish why the order was placed e.g. was it because goods in the inventory are damaged? (see item number A123).

9. Extract a listing of items where date of last sale is (say) more than 9 months (and purchase date is also more than 9 months) prior to masterfile date (30 June 0002) to assist in identifying non-saleable inventory/inventory which should be written down.

10. Extract a listing of items where either the date of last sale or date of last purchase fall after the inventory masterfile date (see connector 7/0002).

11. Extract a random sample of items to be counted at the inventory count (after summarising by location, quantity and value).

12. Cast the value field to obtain the total value of inventory for comparison to the figure used in the trial balance.

THE USE OF MOBILE INFORMATION & COMMUNICATION TECHNOLOGY ON AUDITS

It has been common practice for many years for auditors to "audit with the computer", using laptop computers to perform many of the fundamental tasks they are required to carry out. These laptops have enabling facilities and software that the auditor is able to use to create and store client's audit files, download client trial balances and other financial information, complete workpapers and audit programmes, refer to relevant legislation, standards, complete timesheets and many other tasks. As computers become more and more integrated with communication technology, audit management and their teams are evolving towards being able to communicate to and from remote client locations so that critical audit information is shared instantly, backups to secure central servers can be managed at will, information on the audit firm's office networks can be updated wherever audit staff happen to be and so on. This brings some security issues to light just in the same way as it would if this information were being manually transferred. Before considering security issues, this section looks at how portable information and communication technology assists the modern auditor.

1. WHAT THIS TECHNOLOGY CAN DO

1.1 Planning and administration

* Audit files can be maintained, updated and shared by all members of the audit team.
* Soft copies of engagement letters can be reviewed and updated as needed.
* Available financial data can be communicated to the auditor and charted/graphed/analysed e.g. to assist with the performance of a preliminary analytical review.
* Spreadsheets can be used to produce risk matrices and to document all the factors considered in the assessment of the risk of material misstatement by assertion and determination of planning and performance materiality.
* Copies of standard audit programmes/prior year audit programmes can be tailored as and when necessary, for use on the current engagement.
* Spreadsheets can be used for the preparation of detailed time and money budgets so that actual audit times can be loaded at regular intervals in order to allow audit supervisors to effectively monitor progress and costs.
* Industry specific information can be downloaded from the internet to assist the audit team in gaining an understanding of the entity.

1.2 Obtaining an understanding of internal controls

* Graphics and flowcharting packages facilitate documenting and updating of the auditor's understanding of client systems.
* Soft copies of standard internal control questionnaires (I.C.Qs) can be used to enable client responses to be updated directly onto electronic workpapers.
* Intelligent software and/or exception reporting facilities, can be used to summarise weaknesses identified by the completion of I.C.Qs to facilitate evaluation of audit risk and planning of the audit.
* Expert systems/databases can be used to assist with risk assessments and identifying appropriate audit procedures.
* Management letter points on systems and control weaknesses and drafting of the management letter can be facilitated by integrating audit software, relevant databases and word processing functions.

1.3 Obtaining and Documenting Audit Evidence

* Prior year's work papers and audit programmes, including comparatives where applicable, can be rolled forward and updated in respect of the current audit.
* Audit software can be used to assist with selection of random statistical samples, calculation of appropriate sample sizes and the evaluation of the results.
* Soft copies of confirmation letters can be prepared/updated by audit staff and passed to clients for printing without having to return to the auditor's office.

* Client trial balances can be emailed or downloaded onto memory sticks and audit software can then be used to:
  - create electronic workpapers, and
  - allow for automatic updates to all affected workpapers when audit adjustments are processed.

1.4 Preparation and Review of Financial Statements

* Consolidation modules may be incorporated into audit software to facilitate production of consolidated financial statements.
* Client tax computations/formulae can be automatically checked by use of appropriate programme functions e.g. spreadsheet programmes have such functions.
* Soft copies of standard formats for the presentation of financial statements can be:
  - amended/tailored to suit each client's particular requirements, and
  - integrated with trial balance functions to allow for automatic generation of financial statements.
* Again, use can be made of spreadsheet based financial modelling programmes to assist with the performance of an overall review.

1.5 Application of Generalised Audit Software (GAS.)

* Client files can be saved to disc, memory stick or other storage devices to enable the auditor to apply procedures to the file (e.g. select a monetary unit sample selection from a debtors file).
* A less commonly used possibility is that the auditor's computer can be linked to the client's equipment and used to interrogate client files and perform various audit functions on the files (e.g. check the casts of the fixed asset register).

  Refer to Computer Assisted Audit Techniques for a full discussion on GAS.

2. SECURITY IMPLICATIONS OF USING MOBILE INFORMATION AND COMMUNICATIONS TECHNOLOGY ON AUDITS

The use of such technology on audits brings with it the need for adequate security in two main areas:

* Security over audit "workpapers",

* Security over client information when being interrogated/manipulated or communicated by the auditor .

2.1 Security over "workpapers" - controls to restrict unauthorised access to the firm's computers and storage devices

* All audit staff must be thoroughly briefed on the importance of maintaining the confidentiality of the data on their computers and storage devices.

* Computers should be switched off when not in use and time out facilities should be enabled.

* User ID's and passwords should be required to start up the computers and to access applications. Sound password controls should be adhered to.

* The audit senior should act as a "mobile-librarian" and should be responsible for:
  - ensuring all computers/storage devices left on the client's premises are locked away securely (audit team members will usually be responsible for their own laptops),
  - ensuring backups are taken and kept secure and separate from computers, specially overnight and over weekends,
  - monitoring the use of storage devices by the staff under his supervision,

- returning all storage devices which are no longer required to the audit firm's office.

* Sensitive information, such as evaluations of management, should not be taken to the client's premises at all.

* There should be a library system at the audit office under the control of a designated librarian or administration manager. Sound controls should be put in place including control over the movement of (hardcopy) files and storage devices.

* Controls over files/storage devices should ensure that they are signed out by the person withdrawing them for use.

* All back up copies should be equally well protected.

2.2 Security of client files

Precautions must be taken to prevent destruction of or damage to client files.

* Where possible, copies of the client's files should be made and only the copies accessed.

* Where it is necessary to access the files themselves (e.g. where there is doubt as to whether the copy is the same as the original) then
  - only audit software which has been thoroughly tested by a computer audit specialist should be used,
  - the full procedure should be done in the presence of the client's IT personnel,
  - the software should be "read only" software if possible,
  - access should be restricted to only those files necessary for audit purposes,
  - the client's staff should not have access to the audit software,
  - the client should have "backed-up" to time of access by the auditor.

CHAPTER 9

COMPUTER AUDIT – NETWORKS AND RELATED CONCEPTS

CONTENTS

		Page
INTRODUCTION		
1.	General	9/3
2.	Trends in information technology	9/3
NETWORKS		
1.	Why have them?	9/5
2.	Terminology	9/5
3.	Audit implications of networks	9/6
DATABASES		
1.	What is a database?	9/9
2.	Terminology	9/9
3.	Audit and control implications	9/9
ELECTRONIC MESSAGING SYSTEMS		
1.	Introduction	9/11
2.	An illustration of electronic data interchange	9/11
3.	Audit and control implications of EDI	9/15
4.	Electronic funds transfer	9/16

THE INTERNET

1. What is the Internet? 9/21
2. How is the Internet used commercially? 9/21
3. Risks and controls: trading on the Internet 9/22

COMPUTER BUREAUX

1. Introduction 9/26
2. Audit implications 9/26

VIRUSES

1. What are viruses? 9/28
2. Virus categories 9/28
3. Audit and control implications 9/29

COMPUTERISATION AT PRORIDE (PTY) LTD 9/30

INTRODUCTION

1. GENERAL

The previous chapter dealt with the basics relating to computer auditing. This chapter deals with more complex issues and focuses on environments which are characterised by the presence of data communication i.e. the transfer of data between computers. This type of environment is, as you are aware, all around us. In the workplace computers within departments and between departments, are linked, companies around the country link their various offices and the world has linked itself through the omnipresent Internet.

If we make a simple comparison between a stand alone personal computer used in a small company's accounting department, and a large linked network of computers, it is easy to see that in the latter there is significantly more risk which must be controlled. It is important that controls be implemented to assist in:

* controlling access to computer resources. Remember that where information is transmitted (data communication) there will be numerous computers which are all linked together. It therefore becomes "physically" possible to access the system from numerous points ***and*** to access the system via the communication line (just like tapping a telephone).

* maintaining the integrity and security of data which is being transmitted. It will be of little use if data being transmitted is completely or partially lost, is changed during transmission or its confidentiality is compromised.

At the outset you must realise that the more complex and sophisticated data communication systems are very technical, but that a detailed knowledge of computer science and communications is not required by the "everyday" auditor. Certainly the audit profession, and the large firms in particular, will have employees who are technically excellent and right up to date with developments. What is required by an "everyday" auditor is a general understanding of the risks and controls and the sense to realise that expert knowledge may be required.

Remember also that it is the business world at large which faces these risks, and that there are numerous companies and groupings of companies, such as banks etc, who are continually seeking ways of improving access control, integrity and security in data communication. It is obviously necessary for the audit profession to keep abreast of technological developments, but it is also important that the profession does not lose sight of the fact that the audit objectives do not change.
(See the description of computerisation at ProRide (Pty) Ltd at the end of this chapter.)

2. TRENDS IN INFORMATION TECHNOLOGY (IT)

To the layman it would seem that trends in information technology are geared to speeding up processing, developing smaller storage devices that can store much more data and making computers more user friendly. These, together with developments in communications technology and some other more technical developments, have helped facilitate the ability of businesses to deal in huge transactional volumes and to communicate globally in an instant. Some of these trends are discussed below:

* ***The move from mainframes to personal computers***. This trend is well established, improvements in technology have brought about huge increases in processing power and data storage capacity. As a result there is a move away from centralised data processing units towards "end-user computing" which has significant implications for the internal controls of the company and for the extent to which the auditor can rely on these controls. To be more specific, employees in all sectors of a company have PCs on their desks which potentially give them access to ***all*** of the data, programmes, masterfiles etc. on the system. Division of duties is placed under threat, and data integrity and confidentiality can be compromised if the correct control techniques are not put in place. The auditor has also benefited from the reduction in size of computing devices. It is now

common practice for auditors to use a laptop computer to document their work in electronic workpapers in the field.

* ***Client/server systems architecture.*** The term architecture refers to the way in which the hardware and software is configured or set up. The simplest version of client/server architecture is a local area network (LAN) configured so as to promote the sharing of files, printers and other computer resources.

  Machines which use these resources are known as "clients", and machines which offer these resources are known as "servers". Critical computer resources such as operating systems, application programmes, and data bases are distributed among various processors, which can themselves be scattered throughout the organisation's premises. Again, this has significant internal control implications for the company and the auditor e.g. breakdown in division of duties, integrity and confidentiality of the IT system compromised.

* ***Open systems.*** This term refers to a drive to promote inter-operability and transportability between software and hardware. This aim can only be made possible through the application of common standards among all manufacturers and developers of hardware and software. Open systems result in greater ease of access by all who use resources which comply with open system standards. Again, this has internal control implications for the company and the auditor.

* ***Image processing.*** As computers increase their processing and storage capabilities and become more cost effective, so image processing, e.g. scanning, will become more common place. Where image processing is used, there is increased reliance on the backup of electronic information to prevent the loss of audit trails - again, a particular cause of concern for the auditor.

* ***CDs, DVDs and USB memory devices.*** A number of small effective data storage media devices have developed. These devices present both an opportunity and a threat. They facilitate the sharing of information and facilitate the backup of data. For example, auditors can use these devices to obtain large quantities of data from their clients to analyse or to backup their electronic workpapers when in the field. However, these devices also present a security threat as they make it easy for an unauthorised individual to copy or steal large quantities of sensitive data.

* ***Smartcards.*** A smartcard contains a micro processing chip, as opposed to the magnetic strip of a normal swipe card. Smartcards therefore possess storage space as well as intelligence and can be used to enhance identification and authentication procedures, e.g. through storage of biometric data (like retina scans). The improvements in access control, which are possible through the use of smartcards, have positive implications for the auditor, as better controls over access to the system make the system more secure from both the company's and the auditor's perspective.

* ***Communications technology.*** The last decade has seen rapid advances in communication technologies. Electronic funds transfer (EFT), the Internet, electronic data interchange (EDI), all of which are covered in this chapter, are now common in business. Wireless communication has facilitated mobile business people, for example sales staff, to have access to real time information and to submit orders whilst on the move dealing with customers.

* ***Web enabled.*** Many business applications are becoming "web enabled". This term refers to the ability for users to interface with the application concerned via their web browser. As a result, these applications can be accessed from outside the organisation, i.e. over the Internet.

* ***Cloud computing***. Simplistically, this is the term used to describe the practice of storing a company's (or individual's) data and programmes on a storage device which is remote and which is accessed via the internet. Service providers who offer this service have termed this as "cloud computing". Of course this doesn't mean that the data is stored in a "cloud", but it does mean that it is stored on giant servers in some super secure facility somewhere in the world!

NETWORKS

1. WHY HAVE THEM?

It is thought that networks originated through a desire to share printers among a number of people in an organisation. Instead of having numerous printers (which all cost money), but which lie idle for a lot of the time, it made sense to think of a way to link the users to one printer which could be kept busy for much longer periods of time. This idea has progressed significantly, so that networks are now used to promote the sharing of virtually any resource linked to the network concerned. The term "resource" is used to refer to hardware (such as printers and processors), as well as software (such as application programmes and data base management systems) and data (such as masterfiles and databases).

2. *TERMINOLOGY*

2.1 LAN

A Local Area Network (LAN) is a data communications system, which links a number of independent resources, normally by means of a cable, within a small geographic area (e.g. a building). LANs are commonly used to allow communication and sharing of resources among employees in a particular department or area of a building/organisation.

2.2 WAN

A Wide Area Network (WAN) is similar in concept to a LAN, but extends over a wider geographic area. Usually, additional hardware and software is required, such as bridges, routers and gateways, to make links over a wide area possible.

Additional considerations come into play regarding the communication channels themselves in a WAN, namely:

* whether to use a leased line (a line dedicated solely for electronic communication), or
* whether to use a switched line (a dial-up facility with more subscribers than lines), and
* whether to use lines that communicate in analogue or digital form.
  If in analogue, then modems are necessary for conversion from the digital form used by computers to the analogue form used by telephone lines. If in digital form, then Diginet connections would be used rather than telephone lines.

Each of these options have different implications in terms of cost, security and access control.

. WAN's are commonly used to link an organisation to its remote branches, its service providers (the banks), or its trading partners. (where EDI is used).

2.3 VAN

Value Added Networks (VAN) are ***business entities*** which offer links to the expensive message transmission systems referred to in 2.2. In effect, this service allows numerous companies to share these systems at a fee, rather than having to buy, install and maintain them. The use of VAN's is therefore a necessary and cost effective arrangement for many organisations who wish to communicate electronically with remote sites and independent third parties. A VAN is like a telephone exchange; all telephone subscribers are linked into the exchange and calls are received and distributed from the exchange. A fee is charged for being a member and making use of the service. A VAN works on exactly the same principle.

2.4 VPN

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organisation with the same capabilities, but at a much lower cost. A VPN maintains privacy by creating a secure "tunnel" in the public infrastructure through the use of encryption.

2.5 Internetworks

This is the term used to signify the linking up of LANs, WANs etc. Internetworks exist both within and among organisations. They arise as a result of links from PCs to mainframes, mainframes to other mainframes, LANs to LANs, LANs to WANs, WANs to WANs and many other possible combinations of these linkages. There are many combinations but the risks remain the same; increased opportunity for unauthorised access to the system and all the problems which that brings, as well as the potential for data to be lost or changed during transmission. Hence the validity of the data is also at risk.

2.6 Server

A server is an important part of the network. It is a powerful microcomputer which controls the usage of a particular resource available to the users of the network. The print server controls the use of the printer, the file server controls the use of data files and application programme files so, just as the name suggests, a server "serves" the network with the resource it controls.

2.7 Distributed processing

As the phrase suggests, distributed processing is the distribution or decentralisation of computer processing and storage among devices which share a data communication network. You will realise immediately that in a distributed system, processing (or storage) is not limited to one easily controlled site – it could take place at some remote point or points. Therefore, access control becomes even more important, as does the security of the communication link.

3. AUDIT IMPLICATIONS OF NETWORKS

By now you will have realised that the major areas of concern for the auditor when evaluating the accounting system and related internal controls of a client whose systems are networked, will be access and the security of the networks data communication channel. The auditor is interested in the validity, accuracy and completeness of the data that is produced by the system.

3.1 Access control (Validity)

Each new user who gains access to the computer system of the company, increases the risk of invalid access and hence the risk that the auditor may not be able to rely on the integrity of the client's data or programmes. Invalid access could result, for example, in:

* obtaining confidential information from files including those stored at remote sites
* intercepting data in transmission
* altering or modifying programmes or data
* blocking the flow of data, etc.

The effectiveness of security/access controls are therefore of critical importance to the company and the auditor, and becomes increasingly so, as the client environment:

* becomes more highly networked, and
* tends more towards distributed processing.

Unauthorised access to the network may be gained:

* via a bona fide network PC, or
* via connecting an unauthorised PC to the network (for example plugging a laptop into a network socket).

3.2 Access via network PCs

The greater the number of PCs that are linked to the network, the more points of access to the computer resources there are to be controlled. The way that these are controlled is by the implementation of sound general controls e.g. control environment, policies and guidelines, trustworthy personnel, and more specifically, by strict access controls, both physical and logical.

* ***physical controls*** in networks are more difficult because, by their very nature, networks are spread out. With PCs being dispersed and some perhaps being at remote sites, it is obviously not a matter of placing them all in one room and putting access controls at the door! This does not mean that all physical controls can be ignored; a measure of physical control over the PC can still be achieved by having strong office security. Also it is not uncommon for PCs that are considered to be particularly sensitive to have additional physical security. For example

payroll clerks will normally lock their offices when not in them, to protect confidential information stored on their computers.

* ***logical control*** becomes very important and will be achieved by the implementation of access controls at both system and application level based on:
  - ***identification*** of users
  - ***authentication*** of users and computer resources
  - ***authorisation*** by defining the levels of access to be granted to users and computer resources
  - ***encryption***, scrambling or encoding data to make it unintelligible to unauthorised users
  - ***logging*** which is the recording of time and details of access and access violations for later investigation.

It is worth noting that while the threat of security breaches from external "hackers" is a serious business concern, the auditor is typically more concerned with the controls to prevent internal users (i.e. employees) from performing unauthorised tasks. The majority of frauds tend to be perpetrated internally by employees! The company's computer security personnel will be very concerned about external threats to the company's information system.

3.3 Security of network data communication channels

As networks increase in size and geographical distribution, the opportunities for gaining unauthorised access to the network increases – "hackers" have more communication channels to choose from and longer lines which can be explored for points of vulnerability. Controls over the security of these communication lines or channels are therefore additional areas of concern for the auditor when considering the audit of a networked client. Remember that the communication channel which the company uses will, particularly in the case of wide area networks, be provided and controlled by a service provider, not the company. Despite this there are certain controls which the company can implement or insist upon. Specific controls which may be implemented to reduce the risk of unauthorised access to the network through "hacking" include :

* restricting access to dial-up lines, e.g. telephone line which links a company's computer to its bank's computer. Physical and logical access controls should be in place to ensure that only authorised employees gain access to these lines.
* the use of a "call-back" facility. A "call-back" facility works as follows: when a valid user dials into a computer system and is identified, the computer cuts the connection and immediately redials the number which is stored in the computer for that specific user. This protects the system against "hackers" posing as authorised PCs, because re-connection will be with the authentic terminal rather than the "poser". However, hackers have found ways around this control.
* automatic lockout of a user account after more than three unsuccessful attempts to log in. This would assist in guarding against "hackers" using password cracking programmes to access the network.
* the application of industry standards which ensure that the network is developed and controlled the right way.
* the use of sophisticated ***user authentication techniques*** which are specially designed to cope with the complexities of controlling access in a networked environment where distributed processing takes place.
* the use of ***encryption methods*** to protect sensitive data against access while it is being transmitted e.g. public key, private key.
* the use of network monitoring devices which are able to inspect activity taking place on the network, terminate sessions with vulnerable devices and log unauthorised access.
* a secure network architecture using devices such as firewalls, which help secure networks from external threats and can be used to segregate areas within a network to promote a secure environment.

Do not lose sight of the fact that this is a very technical aspect of computing and that the points above present an overview only.

3.4 Accuracy and completeness of data communications

Obviously anybody transmitting information along a communication line wants it to arrive at the other end in an accurate and complete state. Equally obvious is that all the millions of users around the world cannot do their "own thing". If they did, communication would simply be chaotic. This is resolved by the use of communication protocols which define the requirements, rules and regulations which must be adhered to for the communication of information. The International Standards Organisation which, inter alia, develops the standards by which the international computer community operates, has published a protocol (the Open System Interconnection) which is widely implemented.

Essentially users are in the hands of the service provider, and clearly the accuracy and completeness of data transfer i.e. making sure that data is not lost or damaged and arrives at the correct address, must be of paramount importance to the service provider.

To ensure that information is transmitted successfully between two (or more) computers, software which carries out specific tasks is installed on both (or all) computers. These tasks can be described as:

* ***access control***, linking the devices that send and receive the data
* ***network management***, which controls data traffic to and from the communication devices, routing messages to their proper destination and logging all network activity
* ***data and file transmission***, which controls the transfer of data, files and messages between the various communication devices
* ***error detection and control***, which ensures that the data received is the same as the data sent; and
* ***data security***, which protects the data from unauthorised access during transmission.

DATABASES

1. WHAT IS A DATABASE?

A database is a pool of interrelated data, which is managed, structured and stored in such a way that:

* duplication of data is minimised,
* it contains all necessary information which is needed to provide for sharing of common data among different programmes and users,
* the data is quickly accessible by all authorised users, and
* many users can access the same data simultaneously and will be provided with the same view of the data at any one time, in spite of updates which may be in progress.

A database therefore provides for ***sharing*** of common data among different programmes/users, and so is a prime example of a resource which is particularly suited to a networked environment. Common databases include Microsoft SQL and Oracle.

2. TERMINOLOGY

* A ***Database Administrator (DBA)*** should be appointed to manage the database. Duties include:
  - defining access privileges of database users,
  - design, definition and maintenance of the database, and
  - defining and controlling backup and recovery procedures.

* ***Database structure*** may be hierarchical, network or relational. No further details regarding these structures are considered necessary for a general understanding of audit implications of databases. Most financial database systems are structured as relational databases.

* ***Data ownership*** is a term which relates to the administration of data, rather than the management/administration of the database. Responsibility for defining access and security rules, for specific data elements within the database, is delegated by the DBA to appropriate individuals (e.g. the credit controller may be "data owner" of customer credit limits and therefore responsible for advising the DBA as to who should be granted access privileges to this data). Data ownership therefore promotes the integrity of the database.

* ***Data sharing***. The ability of users involved in different applications to use the same data for different purposes e.g. the quantity on hand information for an item of inventory may be used by the buyer as a basis for purchasing more inventory, whilst the inventory controller may use the same information to produce a "value of inventory on hand" report.

* ***Data Independence***. This means that the data is independent of a specific application. It can be shared by other applications as described in data sharing above.

* ***Datawarehouse*** is a term commonly used for a very large database, which usually consolidates information from a number of different sources (applications) within an organisation and is used to provide management reports.

3. AUDIT AND CONTROL IMPLICATIONS

General controls relating to database systems have a pervasive effect on application processing. It is therefore particularly important that the auditor assesses the degree of reliance which can be placed upon these general controls when auditing database systems:

* the DBA's functions are critical in terms of control of the database, therefore the auditor should review these functions to ensure that they are being adequately performed. Of particular importance in this regard are the concepts of ***data ownership*** and ***access control;*** who has authority to change data, and what access privileges are granted to users?

* the effectiveness and reliability of the database in controlling access and updates should be analysed by the auditor by:
  - using query language (e.g. SQL) and other utilities, and
  - attempting unauthorised access to the database.

  Note: This will be carried out by computer audit specialists.

* definition and implementation of standards for ***programme development/programme changes*** is of great importance in view of the fact that data is shared by so many different users using so many different application programmes. The auditor should therefore assess the adequacy of, and adherence to, such standards.

* Segregation of duties of those who design, implement, operate and use the database is also necessary to promote integrity, accuracy and completeness of the database. Programmers who work on database programmes should, for example, not be involved in updating data on the database. The auditor should assess controls in this regard by inspecting organisational charts and by observation and enquiry of appropriate personnel.

Again, if the above is simplified, it becomes apparent that control over the database comes down to the application of sound general controls with a little added emphasis on programme development/change controls, segregation of duties and, the ever present access controls.

ELECTRONIC MESSAGING SYSTEMS

1. INTRODUCTION

Electronic messaging systems involve communicating, transacting and recording ***electronically*** rather than in the traditional ***paper based*** manner. Two forms of electronic messaging commonly used in business, are Electronic Data Interchange and Electronic Funds Transfer. The term Electronic Data Interchange means the ability of a user to transact or trade electronically with other parties via links between their computer systems. Electronic data interchange can take place using a direct link with another company, or by being a member of a value added network (VAN) or over the Internet. The term Electronic Funds Transfer involves the transfer of money from one account to another on the strength of an electronic instruction.

1.1 Benefits

The characteristics of electronic messaging systems are ***speed, minimal use of paper*** and ***less repetition of data*** which results in a more efficient business practice e.g. lower costs, quicker response times, fewer errors.

1.2 Risks

These include:

* system failure which could result in the business being brought to a standstill, losing customer confidence, failure to meet supply deadlines etc.
* a loss of confidentiality of the data being "interchanged"
* the opportunity to introduce manual controls may be reduced e.g. stopping an invalid payment which has got through the system. An invalid cheque payment can be "stopped" from going through by contacting the bank. An electronic transfer cannot be stopped easily.
* increased reliance on networks and data communications.
* loss of audit trail – no paper!
* difficult legal liability issues e.g. if confidential information about a supplier is obtained illegally off the system at large, who is responsible, company A? company B? the VAN or the communication channel provider?

As with all risks, controls can be put in place to address them and these controls are what the auditor will be interested in.

2. AN ILLUSTRATION OF ELECTRONIC DATA INTERCHANGE

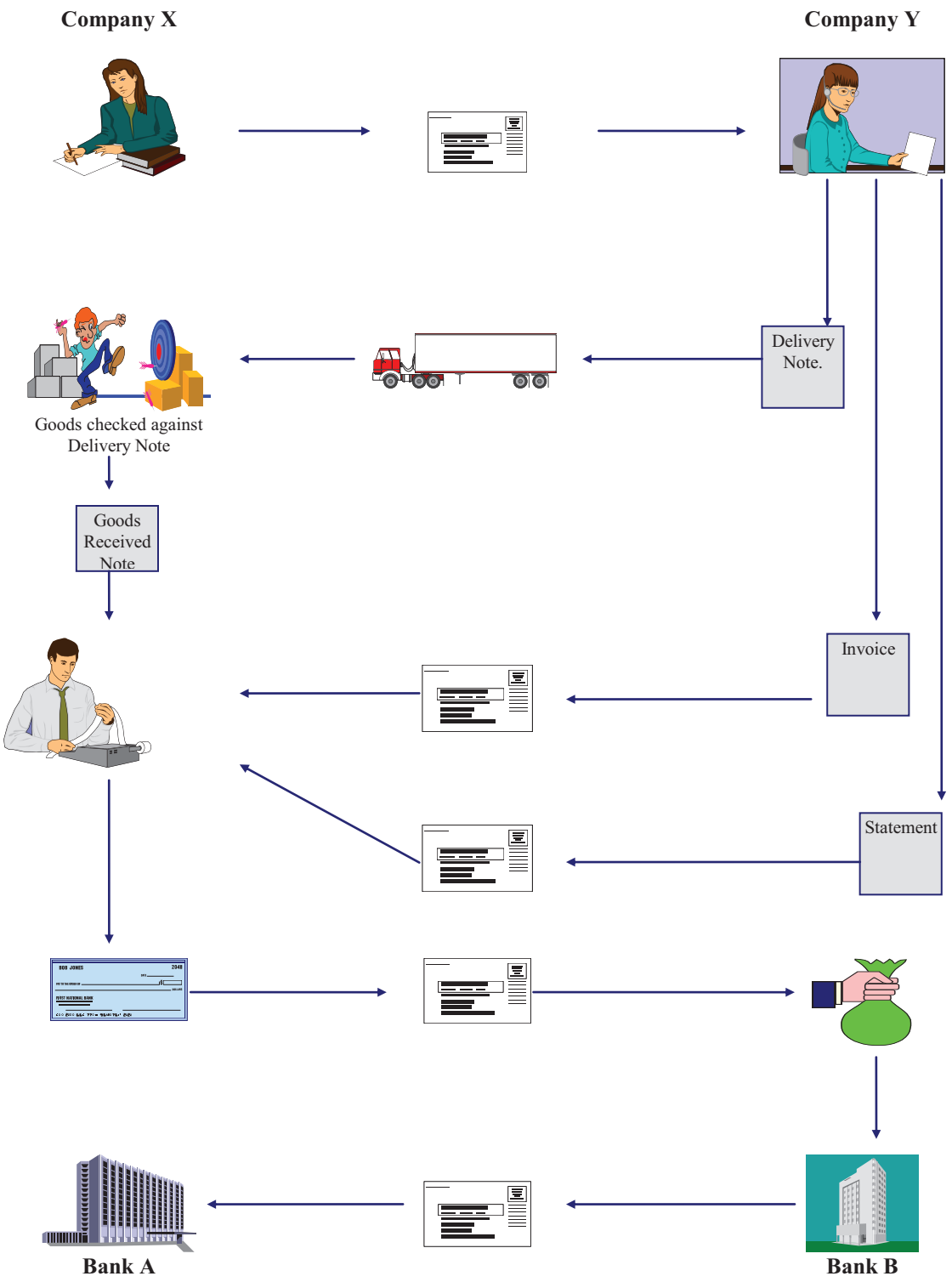
Perhaps all of the above is best illustrated by an example. In the example below, Company X wishes to purchase goods from Company Y. This could be done manually or by using electronic data interchange.

2.1 Without EDI - manually

* Company X will generate a multi-copy order for the goods required, which is then posted to Company Y.
* Company Y, on receipt of the order form from Company X, will recapture the order details onto an internal sales order, will select the goods ordered, and may even then recapture all of these details onto a delivery note.
* The delivery note is then sent together with the goods to Company X.
* When the goods arrive at the premises of Company X, they are checked, and goods which are received in a satisfactory condition, will be signed for and recorded on a goods received note.
* Company Y will then invoice Company X for goods accepted and post the invoice.
* Company X will then probably wait for Company Y to post a monthly statement, before eventually drawing a cheque to pay for the goods purchased.
* The cheque will then be posted to Company Y who will have to bank it with their bank (Bank B), and will record that payment has been received.
* Bank B would have to process and record this cheque and then send it to Company X's bank (Bank A) who would also have to process and record details of the payment.

It is clear in considering the above example that communication of the information relating to each purchase which Company X makes is very slow and that a lot of constant information has to be recaptured at each different stage of the process.

A MANUAL SYSTEM – NO USE MADE OF EDI

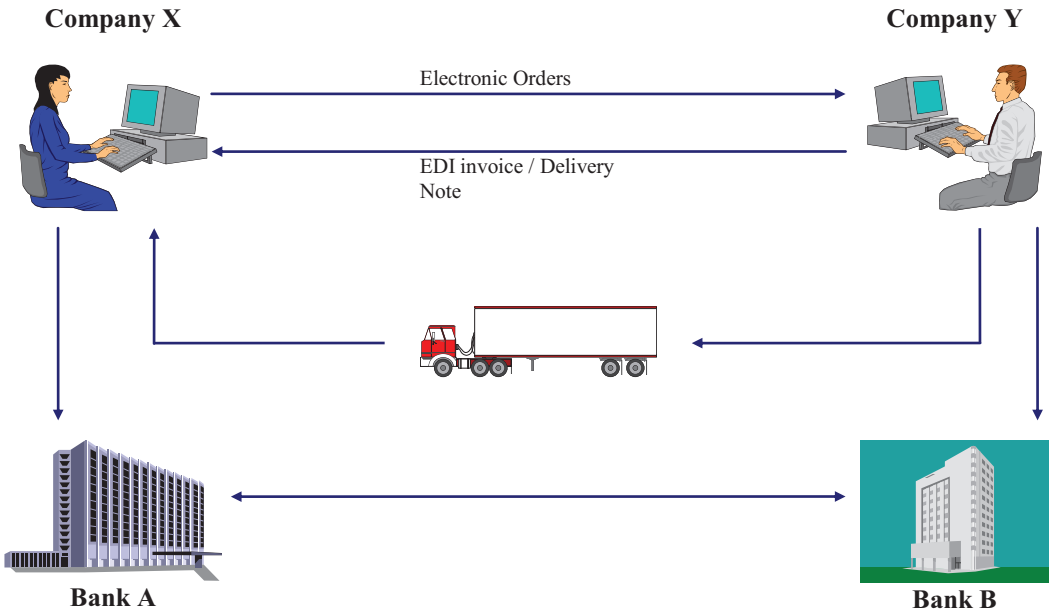


2.2 With EDI

2.2.1 direct links between the companies i.e. not via a VAN

* Company X sends an electronic order via its computer to Company Y's computer.
* Company Y's computer receives the order and generates the necessary instructions to fill it.
* Company Y's computer then adds data such as delivery details and prices before retransmitting the message back to Company X's computer in the form of an electronic invoice.
* Company X then simply adds the date that the goods are received, to this message in order to generate the equivalent of a goods received note.
* Payment would then also take place electronically, with Company Y's computer advising Company X's computer to pay the relevant amount directly into its bank (Bank B).
* Clearing information for the payment would also be communicated electronically between Bank B and Bank A.

WITH EDI : DIRECT LINKS

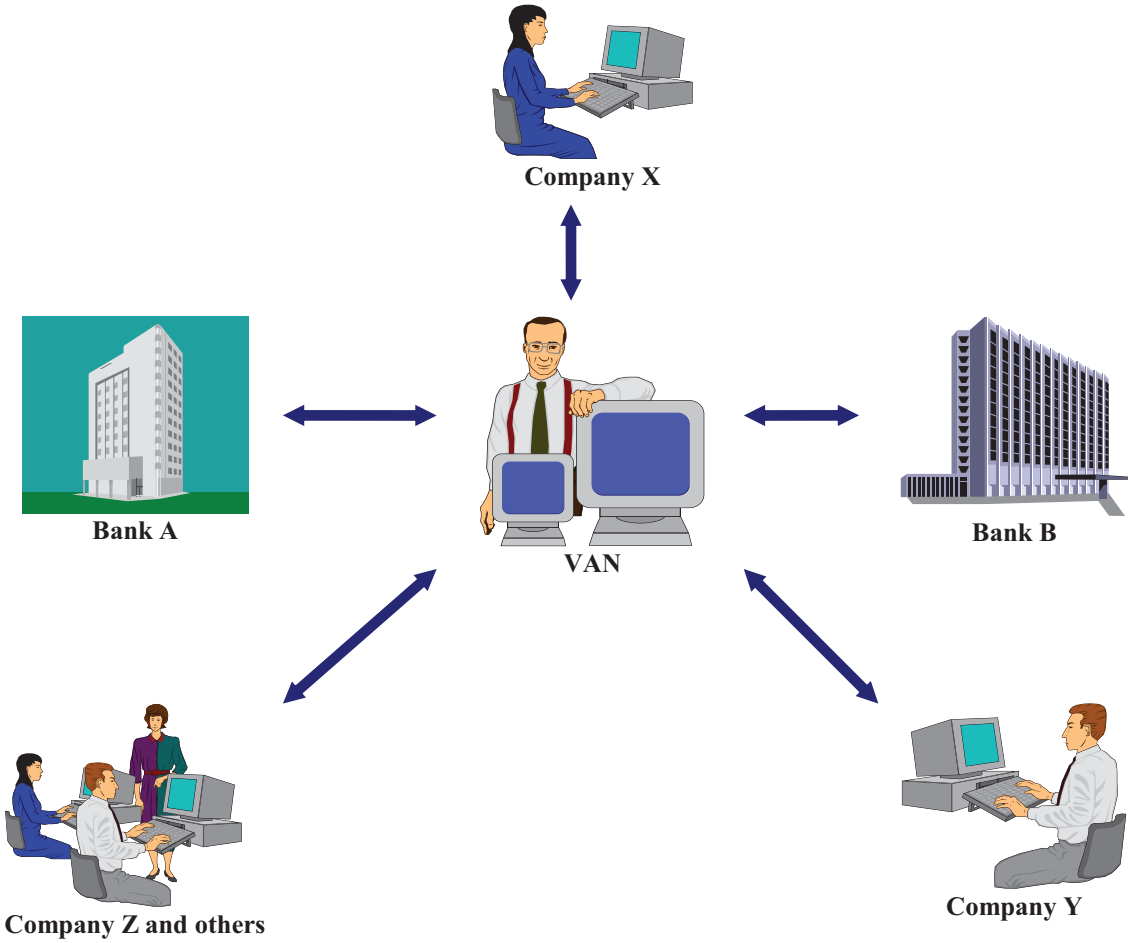


2.2.2 companies linked via a value added network (VAN)

As discussed earlier in the chapter, a VAN is a business entity which offers the service of linking business partners at a central "depot" where electronic messages can be left by one company to be retrieved by another. Companies use VAN's because it would be impractical and very expensive for a business to link itself to all its trading partners and its bank. Where a VAN is used all messages between the EDI partners would still be sent electronically, but they would be sent initially to the VAN. The services provided by the VAN would include :

* resolving any compatibility problems due to differing hardware and software requirements which the different EDI partners may have, and by providing the necessary conversion facilities between systems, protocols, etc.
* provision of a mailbox facility, which allows for storage, forwarding and retrieval of messages sent between EDI partners. The computers of the various EDI partners then simply check their mailboxes at regular intervals to retrieve any messages, which have been sent and stored for them.

WITH EDI: COMPANIES LINKED BY A VALUE ADDED NETWORK



3. *AUDIT AND CONTROL IMPLICATIONS OF EDI*

INTRODUCTION

* The basic requirements of internal control do ***not*** change in an electronic messaging environment. Management must still ensure that transactions are ***complete*** and ***accurately*** recorded and that they are properly authorised (***valid***).
* Many of the conventional general and application controls remain relevant, as is clear from the table below (refer to Ch 8 for more detail on these)
* When considering controls in an electronic messaging environment, the suggested approach is still to: identify risks or objectives and then to determine which control procedures are most appropriate, as illustrated by the table below.

Summary of audit and control implications in an EDI environment

Risk/Objective	*Appropriate Controls*
Implementation of a new EDI system.	* The normal systems development controls apply • Standards specific to the development of new EDI systems should be applied • An ***EDI champion*** (employee) should be appointed by the steering committee to specifically oversee all EDI related matters.
Continuity	* The normal general controls apply here, including: • physical protection, • adequate backups and redundancy, and • disaster recovery plan e.g. revert to a manual system.
Confidentiality/unauthorised access	* Normal access control principles apply. * Access control principles specific to networks should also be implemented (covered earlier in this chapter). * Encryption is of particular importance for sensitive information e.g. user credentials (user names and passwords for authorising transactions).
Fraud/error	* Segregation of duties should be enhanced through physical and logical access controls. * Sound personnel practices should be applied to ensure competent, reliable and honest staff. * Supervisory control should be exercised through the use of supervisory codes to authorise transactions, e.g. after reviewing a transaction which is about to be sent electronically a supervisor adds his personal "code" as evidence of having authorised the transaction.
Loss of manual controls	* Compensating programme controls, e.g. use of check digits on creditors a/c numbers as they are input, reasonableness check on quantities field, missing data checks etc.

Risk/Objective	*Appropriate Controls*
Lack of audit trail	* Parameters within the messaging system should be set to ensure that appropriate use is made of control logs, to compensate for any loss of essential audit trails. * Reports on electronic transactions should be adequate and timely to allow for identification and treatment of problems and errors.
Legal liability	* Use of standard EDI trading contracts to define responsibilities and penalties (see below).
Use of a VAN A company making use of a VAN lays itself open to the risk of unauthorised access to its "mailbox" located at the VAN. However, the company offering the VAN service will want to protect its client's data otherwise it will have very unhappy clients and will go out of business. Subscribers to the VAN expect their data to be protected at all times from unauthorised access, damage, loss or breaches of confidentiality.	Despite the VAN provider's desire to implement and maintain sound controls, users of VAN's should insist upon: * a VAN contract which sets out the responsibilities and duties of the VAN provider and user, which will specify (inter alia): • message content and format details • message acknowledgement requirements • security obligations • details of liability/non performance • validation checks for data received e.g. a reasonableness check on quantity ordered * ***independent*** certification from time-to-time that there is: • adequate control over physical access to storage media at the VAN • strict logical access control • sound back-up and contingency plans • sufficient logging of transactions at each stage of the process • application controls which ensure the completeness and accuracy of data.

4. ELECTRONIC FUNDS TRANSFER (EFT)

As discussed earlier, EFT is an electronic messaging system which transfers money electronically. Most companies currently make extensive use of paying creditors and employees by electronic funds transfer. It is generally regarded to be a far safer method of paying than cheques or cash (wages), but if it is not strictly controlled, the consequences can be very severe. We explain EFT principles in terms of two examples given below.

The procedures for making EFT payments will vary depending on the bank's requirements and the needs of the business. For example, a business which makes a limited number of payments, including once-off payments, will make EFT payments in a slightly different manner to a large business which pays hundreds of employees and creditors each month. The principles will be the same. The essence of the difference is that payments can be made from either a terminal which has been "certificated" i.e. it has certain of the bank's EFT software loaded on it, or from a normal terminal which has no bank software loaded on it. The former will be more suitable for large companies wanting to transfer a file of payments as opposed to a small company wanting to make a few payments including "once off" payments. The following examples will illustrate this :

Example 1

Boomtown (Pty) Ltd a small company, has 30 suppliers which it wants to pay by EFT. It will also need to make 3 or 4 "once off" payments for other items purchased. Not all creditors are paid every month.

1. To set up payment by EFT, the financial manager will have to visit the company's bank and provide extensive evidence of who he is, the existence of the company, his authorisation to use the service, etc. The facility will then be activated specifically for the company's bank account from which EFT payments will be made. He will also provide the bank with his cell phone number.

2. Once the financial manager has set up the facility with the bank, his first task will be to list the 30 suppliers on the system. To do so he will access the bank's site on the internet. He will then log into the website by entering the Boomtown (Pty) Ltd's bank account number and PIN supplied by the bank. If this is successful, the screen will request the entering of a confidential password. On successful entry of the password, the bank's system will automatically send an SMS to the cell phone number provided by the financial manager. This alerts him to the fact that someone has accessed the bank account and is just a precautionary control.

3. Following on-screen instructions, the financial manager creates a list (profile) of the 30 regular suppliers which Boomtown (Pty) Ltd intends to pay by EFT. The list will contain the name and full banking details of the suppliers, e.g. bank, branch, account number.
   3.1 To enter a supplier onto the list (initially or in the future), the financial manager must select the "add beneficiary (payee)" option. At this point the bank's system will send another SMS which contains a "one time" password consisting of numeric and alphabetic characters. This password can be used only once and must be entered by the financial manager for him to be able to add a supplier onto the list of payees (suppliers). Once the list has been created, it remains on the bank's system.

4. When the financial manager actually ***wants to pay*** suppliers on the list, say at the end of the month, he accesses the bank account (gets an SMS to alert him that someone has accessed the account), and following the prompts, selects each supplier to be paid, and enters the amount each is to receive (all the other information, e.g. bank details etc, is already on the system), and sets the transfer in motion by selecting the appropriate option, e.g. proceed, or next. The transfer will then go through.

5. The procedure for making "once-off" payments is slightly different. Once-off payments are made to payees who are ***not*** on the profile and to which the company is unlikely to make regular payments. On accessing the company's bank account (SMS is received as usual), the financial manager will select the "once-off" payment option, and at this point will receive a "one time" password via SMS.
   5.1 Once this password is entered, the financial manager will be taken through a series of screens, onto which he enters details of the payee (beneficiary) and the payee's bank, account number, branch code, reference and amount to be paid.

   5.2 On selecting the "proceed" option, a second "one time" password will be sent via SMS, which the financial manager must enter before the transfer will be activated. Note : two "one time" passwords are required for "once-off" payments as added security.

6. When payments are made in this manner directly via the terminal by an employee, the procedure is independent of the company's financial accounting system in the sense that there is no preparation of a file of EFT payments created on the company's computer system and transferred to the bank as a file.

7. It is important to note that the bank's controls do not prevent the financial manager from adding "invalid" payees, such as himself or an associate in an attempt to defraud the company. The bank requires a PIN and normal password and also adds protection against unauthorised transfers by sending additional "once-off" passwords to a specified cell number, ***but*** it will be the responsibility of Boomtown (Pty) Ltd to make sure that only valid payees are added to the profile and only valid "once-off" payments are made.
   7.1 The risk in this situation arises because of a lack of segregation of duties. The financial manager has access to the PIN and password for the company's bank account and the "one time" passwords come to his cell phone. This lack of segregation of duties will be made worse

if confirmation of the payment is also sent to the financial manager and even more so, if he reconciles the bank statement which may well be what happens in a small company.

7.2 The nature and extent of controls which a company like Boomtown (Pty) Ltd will be able to implement to address this risk, will depend upon the number of employees it has, as segregation of duties will be the best preventive control. Controls over EFT payments should focus on prevention, but must be supported by detective controls. Possible controls are :

- ***Preventive***
  - * all EFT payments should be documented on preprinted, sequenced EFT payment vouchers
  - * each EFT payment voucher should be authorised by two employees (preferably independent of the individual making the EFT payment)
  - * EFT payment vouchers should be sequenced checked, and verified against supporting documentation, before being authorised. The banking details of payees receiving "once off" payments, should be independently verified
  - * the financial manager should log onto the bank's website and an SMS should be sent to his cell phone, but the password to access the facility to make EFTs should ***not*** be known to him. Another senior employee should have this password, and must enter it (note : the financial manager's profile should allow him to do other things on the site, e.g. download bank statements).
  - * the PIN and passwords should be strictly confidential and the financial manager should not leave his cell phone about
  - * a limit on the amount which can be transferred in a single 24 hour period or in a single EFT payment, should be agreed with the bank
  - * the terminal should shut down after 3 unsuccessful attempts to access the bank account/EFT facility
  - * the ability to access the internet should be restricted to the PCs of those employees who need it to do their jobs to the extent that it is practical to do so

- ***Detective***
  - * confirmation of all EFT payments sent by the bank should be printed out, matched to the EFT payment voucher and attached to it
  - * from time to time a senior manager (or the person to whom the financial manager reports), should access the list of payees on the payee file and reconcile it to an audit trail of payees added and/or removed over the preceding period
  - * security violations should be logged and followed up
  - * the cash book reconciliation should be carried out regularly, and by someone independent of the payment process.

Example 2

Marathon Ltd is a wholesale company which pays its creditors by EFT. The company has a large number of creditors.

1. A company which makes a large number of payments would want to prepare a file of payments on their system which they can transfer to the bank over the internet to pay creditors (and salaries).

2. To facilitate this, Marathon Ltd's bank would load its EFT software on a limited number of terminals at Marathon Ltd so that the access to the bank via the terminals is more secure, and the two systems can communicate with each other.

3. Access to the bank's site on the web will be gained in the normal manner via the internet, but once the Marathon Ltd employee gets onto the site, an additional PIN and password, unique to that user, will have to be entered.

4. If this identification and authentication process is accepted, a menu of the functions available will appear e.g.
   - balance enquiry

- download bank statement
- make EFT payment

Access to any of these functions will be directly linked to the employee's user profile, e.g. some employees will be able to download bank statements, and a (very) limited number will be able to make EFT payments. Remember that the employee has already ***identified*** and ***authenticated*** himself to the system, so an additional password may not be required. The employee will then click on the function he requires to exercise his privileges. If the user profile does not allow access to the function "clicked on", either there will be no response and/or a screen message "access denied" will be sent.

5. Obviously the function which has to be most protected is the EFT payment function, and the bank will require that additional controls be implemented.

5.1 The first additional control is to require an additional "password" from the user. This is achieved in different ways by different banks.

Example 1

* a leading bank requires that a (physical) device called a "dongle" be inserted into the USB port of a PC ***which has had the bank's software*** loaded on it
* a dongle is given only to those employees of Marathon Ltd who are authorized to make EFT payments
* the dongle is unique to that employee and must be kept safe and secure at all times. It is in effect a "physical" password which communicates with the bank's software on the terminal.

Example 2

* another leading bank gives the authorized employees at Marathon Ltd a random number generator. This is a small device which provides a "one time" password
* each random number generator is unique to the person to whom it is issued
* the device has its own unique registration number and when it is issued the registration number is linked to the employee's user profile on the bank's software
* once the employee has logged onto the site to make an EFT payment, the screen will request the employee to enter his "one time" password. The employee presses a little button on the device and a random number appears. Remember that the employee has already identified and authenticated himself to the system, so the system can link the random number to the employee who entered it
* of course, the employee must not give his password and number generator to anyone.

5.2 The second additional control is to require ***two*** employees to effect (put in motion) an EFT.

* one employee to ***authorize*** the payment file and another to ***release*** the payment file
* the payment file will not go until both ***authorize*** and ***release*** functions have been activated, and they must happen in the correct order
* once the first employee has selected the authorize option, nobody can write to the file of payments (including the employee who will release the file)
* if the releasing employee requires changes he will have to return the file to the authorizing employee who will make the change and start the process again
* both parties will need to have their own additional password to carry out their functions i.e. the release employee will also have a dongle or a unique random number generator.

6. In addition to the controls over actually making the EFT payment, there must be good controls over the preparation of the file to be transferred. This will be achieved by conventional access controls and careful checking of the content of the file, e.g. confirming payments to creditors against supplier invoices, etc. Of particular importance will be controls over masterfile amendments.

In a large company like Marathon Ltd, control over EFT payments should be very strict. Controls should include:

Preventive

* strict controls over the compilation of the payments file to be transferred, e.g. authority for masterfile changes (adding a creditor, changing a bank account number)
* bank software to be loaded on the minimum number of terminals necessary to facilitate EFT payments efficiently and securely
* only more senior employees to be authorized to effect an EFT
* only a limited number of employees to be given privileges to make EFT payments
* once access to the bank account has been granted, further access should be given on the "least privilege" principle, e.g. some employees can download bank statements but not make payments
* user ID's, PINs, passwords, to be subject to sound password controls (see chapter 8)
* devices such as random number generators and "dongles" to be the responsibility of the authorized employee at all times, e.g. not left with an assistant or left lying about.
* the "two signatory" principles (authorize and release) must be applied
* the terminals on which the EFT software is loaded, should shut down after 3 unsuccessful attempts to access the bank account
* an arrangement may be made with the bank to transfer the money from the company's main bank account to another clearing account and then to be transferred to creditors' (or salary earners') bank accounts. Limiting the accounts to which transfers from the main bank account can be made, protects the main bank account, as attempts to transfer electronically to accounts other than the designated clearing accounts will not be successful
* the amount which can be transferred within a 24 hour period can be limited
* data can be encrypted.

Detective

* a log of authorized access and access violations should be kept and reviewed; problems should be followed up
* an audit trail of all EFT payments should be downloaded the following day and checked against the payments file
* the audit trail should be independently reviewed by a senior official and payments randomly checked against source documentation
* all bank accounts should be regularly reconciled in a timely manner by an employee independent of the EFT function.

THE INTERNET

Use of the Internet for commercial purposes is growing at a phenomenal rate. This has a direct effect on the auditor because more and more audit clients will be making use of the Internet to conduct their normal business activities.

1. WHAT IS THE INTERNET?

The Internet began as a single network (ARPANET) which originated in the U.S.A in the late 1960's as part of a defence research project. It has since been used to connect to hundreds of thousands of other networks in countries throughout the world. It may therefore be described as a huge network of networks all connected together to make up the largest network in the world. Any company which uses the Internet takes on the risks of any network, namely, an increase in the risk of unauthorised access to their own system and its resulting problems including loss of confidentiality, corruption of data and programmes, and the introduction of viruses.

2. HOW IS THE INTERNET USED COMMERCIALLY?

In the same way as a LAN allows employees in an office to share computer resources in that office, the Internet allows users throughout the world to share services and resources made available on millions of computers world wide.

There are a wide variety of services available on the Internet. Different protocols are associated with each service and some protocols are recognised as being more reliable and secure than others. A protocol is simply a standard way of doing things or to be more precise, a set of procedures, requirements and regulations for each service. The most important services, for commercial purposes, include:

2.1 The World Wide Web (WWW)

This is the fastest growing aspect of the Internet and offers the greatest attraction for business. It uses a concept known as hypertext technology to link documents located at different Web sites. These documents are known as Web pages and may include text, graphics, sound and video files. It is controlled by a protocol called ***"http"***, which stands for hypertext transfer protocol. There is a more secure protocol, called "https", that should be used when communicating sensitive information (for example credit card details) – the additional security includes encryption.

Web pages can be used:

* to ***market and advertise products*** to an audience of millions of people;
* to ***offer customers "24 X 7" service*** (ie. Access 24 hours per day, every day of the year to information, products and facilities for placing of orders and/or making payments);
* as a valuable ***source of information*** for businesses, and
* to facilitate the download of "products" e.g. music, articles and information.

2.2 Electronic Mail (email)

Provides users with the ability to communicate quickly and economically, using text or graphics, with other Internet users throughout the world. E-mail is controlled by "smtp", the simple mail transfer protocol.

2.3 File Transfer

This is similar to email, but is used to look for, as well as to transmit, large files as opposed to short email messages. This is controlled by "FTP", "file transfer protocol". Again it is worth noting that there is a more secure, encrypted version, called "SFTP".

2.4 Remote terminal access and command execution

This service allows access to a remote system as if you were on a terminal/PC which was directly attached to that system. Use of this service could therefore provide an organisation with access to powerful processors, large databases, useful programmes and other resources which it may not otherwise be able to access.

3. RISKS AND CONTROLS: TRADING ON THE INTERNET

Let us assume that, in addition to selling its products in the normal way, a company has decided to sell its products over the Internet. Broadly speaking, the company will have to set up a website, design catalogues through which Internet shoppers can browse to establish whether they wish to make purchases, provide a quick and easy way for the order to be placed, and most importantly, have some safe method of being paid for the goods purchased. Trading on the Internet presents a company with a number of different risks which must be controlled. The risks that arise and the control techniques required to address them, are presented below. Remember that, as with all more complex computer issues, there is usually a high level of technical expertise required to understand and implement controls. As a general auditor, you are not expected to have this specialist knowledge but you should have a broad understanding of the risks and how they are controlled.

3.1 ***Risk:*** Any company selling its products over the Internet must comply with the Electronic Communications and Transactions Act. Failure to comply with this Act, which is designed to protect consumers, may well result in the company facing liability.

Control: Appointing/consulting personnel with the necessary legal and computer skills to implement the requirements of the Act ***and*** to monitor compliance on an ongoing basis.

3.2 ***Risk :*** By connecting to the Internet, the company ***creates a channel or link*** to the outside world which could facilitate unauthorised access to the company's computer system. This could lead to service disruption, virus contamination, data destruction or corruption and the loss of confidential information.

Control : A number of controls could apply, including:

* configuring the company's own system to restrict the access which the Internet link provides to only those resources that need to be linked
* processing and storing particularly sensitive applications on separate systems (systems not linked to the Internet), e.g. a computer which is not physically connected to the other computers linked to the Internet
* providing a means of restricting traffic to and from the Internet so that it all has to go through a carefully controlled route. This is achieved by introducing what is termed a ***firewall*** – specialised hardware and software, which is configured with sets of rules, which dictate the permitted protocols and source and destination locations. The firewall is placed between the Internet network and the company's system.
* installing Internet and email monitoring software, for example Web Marshall and Mail Marshall. These products can:
    - log the sites on the WWW which have been accessed by employees (this will dissuade staff from accessing illegal or unacceptable sites from the office, and wasting time on the Internet),
    - prevent users from accessing certain web sites,
    - control the addresses, length and content of emails by monitoring the email protocol (smtp). Thus emails to or from certain specified addresses or over a certain length or containing attachments (e.g. video footage), may not be allowed to pass,
    - pass all incoming files through a virus scanner,
    - encrypt emails which are sent to specific sites,
    - control the delivery of messages to specific PCs.

3.3 ***Risk :*** Orders may be accepted and the goods dispatched but payment may not be received from the customer.

Control : Before the company fills any orders, they need to be satisfied that they are dealing with a genuine customer ***and*** that there is a very high expectation that the customer will pay. Essentially the customer needs to be ***identified and authenticated***. This can be achieved as follows:

* The company can obtain personal details about the client (over the Internet) including citizen identification numbers, or credit card details which can be authenticated. The customer can

then be provided with a password which must be kept secret and used by the customer when placing an order, to identify and authenticate him or herself.

* If further authentication is required, the customer can be subjected to "challenge-response" where, before transacting, the user is required to provide answers to questions about details which were provided when the customer "opened" his account, e.g. what is the name of the family pet? The computer then compares the answer given by the user, to the customer's file.
* An email address can be requested. This provides an additional way of tracing a transaction and also allows the company to contact the address to confirm the order. It is not foolproof, but may alert a person whose email address has been used fraudulently to the transaction.
* Restricting the method of payment to credit card only. The system should obtain clearance on the credit card details supplied by the customer. A direct link with the bank will provide the supplier with confirmation that the card is genuine, not reported stolen or expired and that the account contains the necessary funds. Before the goods are despatched, the funds transfer should have been authorised. Of course genuine card details do not mean that the owner of the card consented to its use (it may have been stolen) but that is the concern of the card owner. Passwords, pins and cards must always be kept secure. An additional point to remember is that if a person is trying to obtain goods fraudulently over the Internet, he has to gain physical access to the goods so a delivery address must be provided. This will leave a trail but it will be time consuming and costly to follow this up if the sale proves to be fraudulent. It is far more efficient to prevent the situation from arising.

Note: A company trading over the Internet may accept orders from a customer and charge the sale to the customer's account (i.e. like a normal credit sales/debtors transaction). In this case all the normal controls for extending credit should be adhered to e.g. creditworthiness checks, credit limits, as well as identification and authorisation of the user prior to accepting the order.

3.4 ***Risk :*** Information keyed in by the customer may be inaccurate or incomplete, resulting in orders which cannot be filled, e.g. if the customer does not indicate the quantity required, the order can't be filled. This will lead to customer dissatisfaction and lost sales.

Control : This risk is reduced (eliminated) with adequate input validation and reasonableness checks, for example web pages which:

* Are properly designed to display spaces for all information required and are easy to follow.
* Require the customer to key in the absolute minimum, e.g. instead of keying in the description of the item required, the customer will simply select and "click" against a list of goods available which appears on the screen (drop down lists).
* Contain programme checks which enhance accuracy and completeness, e.g. alphanumeric on number fields and a ***mandatory field*** check on the quantity ordered field where an item has been selected.
* All other information, e.g. item number pertaining to the item ordered, will be linked to the description and will not have to be entered.

3.5 ***Risk :*** Unauthorised disclosure of confidential customer information (by hacking, eavesdropping) and/or loss of data integrity (data is changed in some way), once transmission of the transaction is underway.

Control : The inclusion and enabling of transport layer security techniques (e.g. secure socket layer) which:

* Encrypts sensitive data to ensure confidentiality.
* Authenticates the user (thus ensuring authorised access).
* Implements programmed checking which tests the completeness of data as well as testing for any changes thereto (integrity), e.g. details of the order are relayed back (on screen) to the customer by the sales system for final acceptance. Customer is required to "select and click" on desired option e.g. "confirm amount" or "cancel".
* Transaction logs and transmission logs are produced and reviewed to ensure that all transactions sent, were received.

3.6 ***Risk :*** Potential customers may be lost (and the reputation of the company damaged) if customers are not satisfied that the website does not contain malicious code or content, and that the company is a legitimate business.

Control:

* Confidence in the site can be enhanced by having the site verified (on an ongoing basis) by a reputable certificate provider e.g. Thawte, Verisign, and displaying the company's privacy policy on the site.

* Web applications should be designed to be secure. Adequate input validation, reasonableness checks and user authentication techniques must be implemented. This is a highly specialised area where specialists should be used.

3.7 ***Risk :*** By selling over the Internet the company becomes a 24 hour a day, 7 day a week, 365 days a year business. Any lack of availability or functioning of the site will result in lost sales and may affect the company's reputation.

Control : A reputable service provider must be used and the company must employ staff with the necessary computer and website maintenance skills to ensure that the website is available and fully functional at all times (and that the website is up to date, attractive and user friendly). Adequate redundancy and disaster recovery commensurate with the needs of the business / web site should be implemented.

3.8 ***Risk*** : The consequences of incorrect pricing become more significant:

* As the company does not only sell its products via the Internet, it may be in competition with itself. For example if it sells through retail outlets, the Internet price must not be so favourable that retail suppliers are compromised, or that overall profitability is reduced.
* If the true costs of selling over the Internet are not carefully identified before setting Internet prices, overall profitability may be compromised (i.e. the selling price of Internet products are set too low).

Control : The company must employ staff with the necessary competence, and implement information systems which provide these staff with the ability to:

* Set selling prices for all products (whether they are sold over the Internet or by other means) which optimise sustained profitability.
* Identify all costs which are applicable to the Internet business e.g. transport/delivery, additional staff, warehousing, on an ongoing basis.

3.9 ***Risk :*** Unless the website in some way restricts the geographical areas to which Internet sales can be made (e.g. South Africa only) the company will face the risks of international trade. The company may:

* Unknowingly contravene export regulations (and import regulations of other countries).
* Unknowingly contravene financial export regulations.
* Fail to meet customer expectation due to a poor delivery service (too slow, unreliable etc) thereby damaging the reputation of the company.

3.10 ***Control*** : Again the response to this risk would be to employ staff who have the necessary expertise, and implement and monitor on an ongoing basis, policies and procedures which can cope with these additional risks, e.g. a separate department may be set up, headed by a competent Internet trading manager, and all deliveries would be handled by a single reputable international courier service.
Note: Even if the company does not sell outside the country's borders, if the delivery method e.g. courier, postal service does not meet customer expectation, the business will suffer loss of sales.

3.11 ***Risk :*** An inadequate audit trail may hinder the company's ability to defend itself against legitimate or fictitious claims or queries pertaining to a transaction e.g.

* Repudiation – the customer denies having placed the order.
* The customer claims to have placed an order which was not filled.

Control : The methods which are used to prevent repudiation, are all reasonably complex and are beyond the scope of this text. However, the control techniques which can be put in place for the company to defend itself against both repudiation and customer claims, include the use of:

* Digital signatures (a unique mark which only the sender of the message can make and which is attached to the message and can be recognized or authenticated by another party).
* Time stamping (which identifies the date and time of the message so it cannot be refuted).
* Having software which provides a comprehensive audit trail consisting of transaction logs, transmission logs, system activity logs which record all stages of the transaction; this is perhaps the best defence.

Remember: There are numerous other aspects of the cycle which must still be controlled by conventional means. In effect, selling over the Internet is just a revenue and receipts cycle with a difference. In our example of selling over the Internet, once the order has been received, it must still be picked, packed and despatched. Inventory must still be safeguarded, goods purchased for sale must still be properly ordered, received and recorded, salaries and wages must still be paid. Conventional manual and computerised application controls will still be required.

COMPUTER BUREAUX

1. INTRODUCTION

A computer bureau is a business entity which processes other entities' data for a fee. The bureau provides the necessary hardware, software and skills to perform the function. This may be appealing to certain companies as it means that they do not have to outlay money for equipment and computer staff.

A bureau may provide a number of different levels of service, including:

1.1 ***Facilities management*** – in which computers are housed at the bureau and the bureau staff may provide infrastructure support for the hardware, operating system and database, but applications are managed by the business itself.

1.2 ***Application service providers (ASPs)*** – the entire service related to a particular application is provided by the bureau.

1.3 ***Full outsourcing*** – in which case all IT services are provided by the bureau.

Some companies use bureaux to enhance confidentiality of sensitive information e.g. salaries may be processed off site by a bureau.

In essence the use of a bureau simply means that a stage in the accounting process does not take place at the client, but at a separate business entity. However:

* Data must still be ***input,***
* Data must still be ***processed,***
* ***Output*** will still be created.

It follows therefore that controls over each of these functions must still be maintained but that the responsibility for the controls in each function will depend upon whether the client or the bureau is performing the function.

2. AUDIT IMPLICATIONS

As indicated above, when a company uses a bureau it is adding another dimension to the accounting system which will need to be controlled. The auditor, in formulating his audit strategy and plan, will need to evaluate the controls over the use of the bureau. Ultimately he needs to determine whether the accounting system, of which the bureau is now a part, and related internal controls, will provide ***valid, accurate*** and ***complete*** data. Of course it is in the interests of the client and the bureau to provide precisely that, but the auditor cannot rely on this and will therefore need to evaluate the bureau's role.

It is very unlikely that the bureau is going to allow the auditors of all its clients to come in and perform an indepth evaluation of its general and application controls, as to do so would be impractical and inconvenient. At the same time the auditor cannot simply disregard the bureau's role. The auditor's assessment of the bureau will probably be centred around:

2.1 ***An assessment of the bureau's suitability***

The use of a bureau by a client is, for the auditor, similar to relying on an expert. Hence the auditor should assess the professional reputation of the bureau including:

* its competence,
* its independence in relation to the auditor's client,
* its stability,
* the range of services offered to the client,
* the reputation for confidentiality the bureau enjoys,
* the security arrangements the bureau employs to safeguard the integrity of the clients' files, reports and programmes,
* its efficiency and reliability in meeting deadlines,
* its ability to service the client using the most reliable and up to date computer developments.

It is not always easy for the auditor to assess the above, but he should make the best use possible of trade publications, professional bodies to which the bureau may belong, and discussions with the client and other users as well as a review of correspondence between the client and bureau which may provide evidence of

the above. The auditor should also observe the relationship between his client and the bureau to gain the above insights.

Some bureaux will arrange independent evaluations of their business from time to time. It is in their interests to do so as the evaluation report can be used to promote the bureau. If such an evaluation exists, the auditors of the bureaux's clients should make use of it e.g. a report, which provides an independent opinion on the operating effectiveness of the key controls operating at the bureau. See page 17/25.

2.2 An evaluation of the bureau agreement

This agreement is very important as it defines the responsibilities of the client and bureau and will be the primary source of reference in any dispute. It should cover the following:

* Identification of liaison personnel and their authority, at both the bureau and the client e.g. if there is a problem, who is contacted?
* A description of :
  - the input to be provided,
  - the processes to be performed,
  - the output.
* Deadlines for input and output delivery, and the procedures and consequences of these deadlines not being met.
* Client responsibility in respect of :
  - data preparation,
  - input control,
  - masterfile amendments – how do they happen and how are they authorised etc?
* Bureau responsibility in respect of :
  - data acceptance,
  - handling errors,
  - notifying client of system changes/programme developments.
* Back-up processing arrangements,
* Ownership of data files, programmes and documentation,
* Liability of the bureau for loss of data in any of its forms (e.g. files, input documents),
* The term, renewal options and cancellation of the agreement,
* Basis of fee charging for various services offered,
* Insurance cover for the bureau,
* Fidelity insurance for bureau employees,
* Disaster recovery plans,
* The access the auditor might or might not be entitled to,
* Training and support of client personnel who interact with the bureau.

Typically these agreements include formalised service levels. These service levels are often reported against in monthly reports. In many cases there are penalty clauses for non compliance with the contracted service levels.

2.3 An evaluation of the controls put in place at the client over the functions which are the responsibility of the client

This will involve performing conventional tests of controls, (observation, enquiry, inspection, etc) over the functions which are the responsibility of the client, e.g. gathering data for processing or reconciling output.

Again remember that the use of a bureau takes care of only certain functions within a cycle, the other functions must still be controlled as they would be if computing took place at the company itself. For example, a bureau may process a client's wages but the client is still responsible for the personnel function, timekeeping, and possibly making the relevant EFT payments to employees, all of which will still be evaluated and tested by the auditor. Equally, substantive tests will still be performed as required on transactions, balances and totals.

VIRUSES

Viruses are possible in virtually any computer environment but the risk is increased in highly networked end-user computing environments, (especially the Internet) in which large numbers of relatively uninformed users, who are not adequately control conscious, have access to computer resources.

1. WHAT ARE VIRUSES?

A virus is a computer programme that spreads from one system to another, eventually performing the illicit function for which it was designed. Each reproduced virus works independently of the initial virus. It is common for viruses to be transmitted via email.

2. VIRUS CATEGORIES

2.1 Destructive viruses

* ***Massive destruction*****:** attacks the format of storage devices, whereby any programme or data damaged will not be recoverable.
* ***Partial destruction*****:** erasure or modification of a specific portion of a storage device, affecting any files stored in that portion.
* ***Selective destruction*****:** erasure or modification of specific files or file groups.
* ***Random havoc*****:** random changes to stored data during normal programme execution, or changes to key stroke values, or data from other input/output devices.
* ***Network saturation*****:** systematic demands on computer memory or space to impede performance or cause the system to crash.

2.2 Non-destructive viruses

* ***Annoyance*****:** displaying messages, changing display colours, changing keystroke values (e.g. changing the effect of the SHIFT/ALT keys), deleting characters displayed on a visual display.

2.3 Kinds of virus

Viruses or "malicious code" as they are sometimes called are also described in terms of their capability. Some examples follow:

* Trojan horse - code which results in the performance of an additional function which is unexpected and unknown to the user e.g. copies passwords as they are entered by users.
* Logic or time bomb - code which sets off an action when a specific condition or date occurs, e.g. "on 1 April delete ..."
* Trapdoor - code which allows access other than in the conventional manner (almost like a secret password).
* Worm - code which spreads itself through a network.
* Spyware - a programme which "steals" information from the system on which it is running, such as user names, passwords, credit card numbers, etc.

2.4 Spam, phishing and pharming

Spam "attacks" email systems. The intention is to send so many useless emails to an address that the system crashes (gets saturated). This is also termed denial of service attack.

Phishing is the practice of sending emails to users in an attempt to get the recipient to give away some confidential information, e.g. confirm a bank account number and password. The email is worded and (visually) made to look very authentic and genuine but is in affect a bogus email. Many people are however, fooled and respond.

Pharming is the illegal practice of re-directing a website's traffic which may include confidential information from the official website to an alternate site, and is a major threat to the e-commerce and on-line banking.

3. AUDIT AND CONTROL IMPLICATIONS

A security system which includes the following controls should be implemented:

* All software and data files should be backed up at regular intervals - if a virus causes destruction this will facilitate the rebuilding process,
* Anti-virus software, which is regularly updated with the latest virus definitions, should be loaded on all PCs,
* Anti-virus software should also be used to scan all email entering and exiting an organisation's network,
* Only software from reputable suppliers should be used,
* All users should be informed of the need for data security, and of the potential threats which viruses pose to the integrity of their data, e.g. spam, phishing,
* All purchased software should be carefully examined before use. New software should be loaded onto an isolated PC which contains no critical or sensitive files,
* Access to PCs should be restricted to authorised personnel who should be accountable for their PCs,
* Instructions to users not to open e-mails received from unknown or suspicious sources,
* Installation of anti-spam systems and education of users.

COMPUTERISATION AT PRORIDE (PTY) LTD

1. INTRODUCTION

The following paragraphs describe the computer environment at ProRide (Pty) Ltd, a company which currently operates in South Africa. We have changed its name and the names of its employees, but have described its computerisation as well as its cycles as they actually are. Some of the finer details have been omitted as they are not necessary for an understanding of the company's systems. There are instances where it appears from a theoretical perspective, that controls and procedures could be carried out differently and that possibly even more use could be made of the capabilities of the computer, but bear in mind that theory does not always take into account the practical issues of actually running a business. In addition, there are numerous reports which are produced by the system which we have not even mentioned as they are not central to the operation of the cycles and are used to a great extent in the monitoring and review of the operation of the cycles. What you can accept is that the company runs very efficiently and the extent of computerisation and the controls and procedures which are in place, work very well for the company. The descriptions of the cycles do illustrate how manual (user) controls and programme (automated) controls combine in the various applications and that hardcopy documents are also combined with electronic data. In addition, there are plenty of examples of various types of control activity which you have studied, including physical and logical access controls, division of duties, isolation of responsibility and input and output controls such as minimum entry, screen aids, mandatory fields, matching, etc. We hope that these descriptions will paint a clearer picture for you.

2. BACKGROUND TO THE COMPANY

The company wholesales bicycles and related products e.g. spares and accessories. The vast majority of its inventory is imported from China, Japan or Taiwan but inventory is also sourced from local suppliers. As with most wholesale businesses, inventory is the heart of the business with many millions of rand invested in inventory at any one time. The company is very well run with close attention given to all the components of internal control. Senior management by its actions, sets a tone of control consciousness. With regard to risk assessment, the directors meet regularly to specifically address the risks facing the company. These usually hinge around competition coming into the market place, the focus the company should have, e.g. whether the company should concentrate on "top end" bicycles (high profit margin/limited sales) or "bottom end" bicycles (low margin/high sales) and risks posed by suppliers which are generally located in China, Japan and Taiwan. The company employs enough staff to ensure a sound division of duties and also ensures that its staff are competent to perform their functions efficiently and effectively. A high premium is placed on having information available to make decisions and monitor performance. The company has therefore invested in excellent software (JD Edwards) and the appropriate hardware. This suite of software is one of a number of sophisticated software packages which are termed "enterprise resource planning" (ERP) systems. Other well known ones are SAP, PeopleSoft and Oracle.

Because the company imports its inventory by sea in containers it is convenient for it to be located in a harbour city. The company does not have a large number of suppliers, but does have in excess of 2 000 customers, all of whom are account holders (debtors). The company does not sell to the general public. Its major customers are the chainstores e.g. Makro, but it does supply numerous independent bicycle retailers and "general dealers" in small towns and rural areas. The company makes use of product catalogues which are sent to customers to market its product. The company also employs marketing staff who promote the company's products, keep customers happy etc. Marketing staff do not take orders. As explained in chapter 10 orders are placed by email, fax, phone or post.

The company has about 60 employees, the majority of whom are engaged in warehousing activities i.e. receiving and dispatching inventory, as well as picking inventory items to make up orders and packing/maintaining the physical inventory in the warehouse.

3. THE COMPUTER ENVIRONMENT

Data processing is partially centralised with terminal links to the user departments and partially networked. The company is also linked to the Internet.

3.1 Partial centralisation with links to the user departments

The company has a dedicated computer room which is access protected by a simple keypad system. Access to this room is restricted on a "need to enter" basis. No special physical or environmental protection controls, other than air conditioning, have been put in place. This room houses the IBM AS400 computer on which the JD Edwards software is run, as well as two printers, and two PCs. The company has 4 distinct user departments, namely

* Accounting headed by Johan Els (financial manager)
* Warehousing headed by Reg Gaard (warehouse manager)
* Purchases/creditors headed by Ruth Taylor (purchases manager)
* Sales/debtors headed by Judith Oldman (credit manager)

All user departments are connected to the AS400. The financial director (Brandon Nel) and managing director (Peter Hutton) are also connected to the AS 400 via their PCs, as is Gary Powell the IT manager.

Although ProRide (Pty) Ltd uses JD Edwards software, it has ***not*** purchased all of the modules on offer.

Module	acquired	***Not*** acquired
Sales	√	
Debtors	√	
Inventory	√	
General ledger	√	
Purchases		√
Creditors		√
Cash book		√
Fixed assets		√
Payroll		√

The reason for this is that the sales, debtors and inventory applications are very dependent on each other ***and*** they are needed to provide "real time" (up to the minute) information about the revenue and receipts cycle, as well as the inventory cycle. Control of inventory is considered to be the key to running the business and the management of the company's debtors (cashflow) is of paramount importance. So what about purchases? An up to the minute perpetual inventory requires up to date entry of purchases. This is absolutely correct, but in the case of ProRide (Pty) Ltd, which does not have a ***great number of creditors*** and does not ***make frequent purchases***, it is not necessary to have the purchases/creditors software integrated on the system. Because ProRide (Pty) Ltd imports its trading inventory in large consignments, relatively few large deliveries as opposed to numerous small purchases with frequent delivery are made. When deliveries are made the items purchased are entered into the ***inventory masterfile*** on the AS 400 very promptly, to keep the inventory "real-time". However, the purchases/creditors are ***not*** run on the AS 400 system, they are recorded independently (see 3.2 below).

The same principle applies to cash book, fixed assets and payroll – there are so few transactions that integrating the JD Edwards software for these applications is considered to be too costly and unnecessary.

3.2 Network

The company also has a small local area network (LAN) which links the PCs in the purchases department, the accounting department, the financial manager (Johan Els), the financial director (Brandon Nel) and the managing director (Peter Hutton) and the IT manager (Gary Powell). Resident on this network is the payroll, purchases/creditors, cash and fixed asset software. The payroll, fixed asset and cash book applications are run on purchased package software, whilst the purchases/creditors application was developed some years ago, by Gary Powell (IT manager), to meet the specific needs of ProRide (Pty) Ltd.

Physical access to the PCs on this network is limited as the company's offices are "open plan" other than for senior management who have private offices. These offices are locked overnight and at week ends.

Access to the system and to the application software is restricted by user identification and passwords and the various privileges given to employees are reflected in user profiles as normal. Access is granted on the "least privilege/need to know" basis i.e. access is given to only those aspects of the application which the employee requires to fulfil his or her function. Interestingly, no write access at all is given to either Brandon Nel (financial director) or Peter Hutton (managing director), they have read access only.

Access tables, user profiles and terminal profiles etc, are compiled and maintained by Gary Powell (IT manager) and reviewed regularly by the external computer auditors.

3.3 Connection to the Internet

The company is also connected to the Internet. This gives those staff members who need it, access to e-mail and the world wide web. Non business use of the "web" is strongly discouraged. The link to the Internet does not pass through a firewall as this is deemed an unnecessary cost. A measure of protection is offered by antivirus software, but the company does not believe that by excluding a firewall, they are exposing themselves to much risk.

Besides the use of e-mail, the major use of the Internet connection is for the company to obtain information from its bank (Standard) about its account and to effect electronic funds transfers.

* Bank statements are downloaded daily by the accounting/debtors department so that direct deposits and electronic transfers into ProRide (Pty) Ltd's account from debtors can be recorded.

* Enquiries about specific payments or deposits can be made and the bank account balance can be monitored on a daily basis.

* Salaries, wages and local creditors are paid by EFT.

The connection via the Internet to the bank account is protected as follows:

* The necessary software has been installed by Standard Bank on (only) three PCs at ProRide (Pty) Ltd. These are the PCs of
  - Johan Els the financial manager
  - Judith Oldman the credit manager
  - Brandon Nel the financial director.

* To gain access to the bank's website, the employee will log on to the system by entering user ID and password, and selecting the Standard Bank icon on the screen.

* This will take the employee to the Standard Bank site, but to enter ProRide (Pty) Ltd's bank account, the employee will be required to enter an additional unique password
  - this will bring up a menu of the functions on the website which are available to that employee as described above
  - in the case of ProRide (Pty) Ltd, this is simple. Johan Els and Brandon Nel can access all of the functions whilst Judith Oldman can download bank statements and make enquiries but cannot play any part in EFT payments.

* ***To effect an EFT payment*** the bank requires that an additional "one-time" password be entered. This number is produced by a random number generating device (see page 9/19 for a description of this)
  - Johan Els and Brandon Nel have been issued with random number generators, as has Gary Powell the IT manager, as back-up. (The EFT software is not loaded on his PC as he does not need a link to the bank. He will only need to generate an additional "one-time" password in an emergency when standing in for Johan Els or Brandon Nel).

* In addition to requiring additional one-time passwords, the bank requires that the EFT payment be approved by two employees, one to "authorise" the payment and the second to "release" the payment
  - both employees will be required to enter a "one-time" password generated by their unique random number generator devices
  - in the case of ProRide (Pty) Ltd, Johan Els "authorises" and Brandon Nel "releases".

* The connection to the bank is also protected by automatic shut down of the terminal after three unsuccessful attempts to access the site and logging of access violations. Obviously strict controls over the confidentiality of passwords and the safe-keeping of the random number generator devices are in place.

4. PERSONNEL

The IT department is headed up by Gary Powell who is in charge of all aspects relating to the computerisation of ProRide (Pty) Ltd's information systems. He is well qualified and has a wealth of experience. He has been trained in the use of JD Edwards software and is a competent business analyst and programmer. The in-house programmes used by ProRide (Pty) Ltd (e.g. purchases/creditors) were written by him some years ago.

The only person who answers directly to him is Rushda Devon who is responsible for some data entry, e.g. sales, and other minor accounting and computer functions.

Dalene Burger, the accounting supervisor reports to Johan Els (financial manager), but is located in the computer department as she works closely with the applications on the AS400. She is also very experienced in both computing and accounting. She is also trained in the use of JD Edwards software and the other software used by the company.

Gary Powell works closely with the computer audit partner of the company's auditors. In addition to assisting him with computer problems which arise (very seldom), the audit firm carries out an external review of the system every two years.

The JD Edwards software as well as the other packages used by the company are strongly supported by their suppliers, both reputable computer consultancies. All employees who make use of the system are trained and kept up to date with changes and developments in the software.

5. DOCUMENT MOVEMENT AND DATA ENTRY

5.1 Document movement

Although there is movement of documents between departments (for example internal sales orders from the order department to data capture in the computer department and picking slips between data capture and the warehouse department), a batch system is not used to control document movement. The reason for this is that to keep the system right up to date, ProRide (Pty) Ltd attempts to process transactions "as they happen" almost as in a "real-time" system. Control over document movement is kept by the use of sequenced documentation and, what are termed, "day end reports". At the end of the day, reports are generated which:

* indicate any missing numbers in the source document sequence
* indicate details of the transactions entered, including document count totals and financial totals, if applicable. The "day end reports" are checked the following morning to source documentation. In effect they are transaction journals e.g. the daily sales journal.

5.2 Data entry

As indicated earlier, the user departments are linked to the AS 400. Whilst sales orders and credit notes are entered by Rushda Devon from her terminal in the computer department (see Chapter 10 for a description of this), other transactions are entered via PCs in the user departments, e.g. receipts from debtors are entered from a terminal in the debtors department. Although access to the various application programmes is controlled through user profiles, there is some control exercised by terminal IDs and profiles. For example, access to the salary software cannot be gained from a terminal in the warehouse department even if Johan Els who has the necessary access privileges to the salary application, attempts to gain access.

5.3 Programme input controls

The software used includes a good range of programme (automated) controls to enhance the validity, accuracy and completeness of data entry, for example:

* alphanumerics
* screen formatting and screen dialogue

* mandatory fields – e.g. quantity field on entry of internal sales orders
* validation checks e.g. an internal sales order will not be generated if an incorrect debtors account number is entered
* matching – e.g. on receipt of a delivery from a supplier, the purchase order number on the supplier delivery note is entered and matched against the list of purchase orders awaiting delivery on the system
* the principle of minimum entry e.g. when the details from an internal sales order are entered, the entry of the account number will bring up all the other details pertaining to the customer, and the entry of an inventory item code will bring up the description of the item ordered.

6. AMENDMENTS TO MASTERFILES

A great deal of importance is placed on allocating access privileges to the various masterfiles. Four levels of privilege are possible and are essentially an extension of read only and write access privileges. They are designated as follows:

A	**=**	***add***
C	**=**	***change***
D	**=**	***delete***
I	**=**	***inquire***

A privilege : enables employees to add a record to a masterfile, for example adding a new customer to the debtors masterfile, or adding a new supplier to the creditors masterfile. This is an important privilege particularly in respect of masterfiles which are central to payments made by the company. For example, if controls over the addition of a supplier to the creditors masterfile are not strict, it makes it possible to set up a scheme to make fictitious payments. Up until a few years ago, the add privilege was only allocated to two employees, the IT manager and the accounting supervisor. This has proved to be impractical and the "A" privilege is now given to senior personnel who work with the masterfiles. For example, the payroll administrator can add a new employee to the wage employee masterfile, and Judith Oldman the credit manager can add a new customer. The exception is that the warehouse manager is not given any write access to the inventory masterfile as this enhances division of duties relating to custody and recording of inventory. Adding to the masterfile still requires that the addition be approved before it is entered and all amendments are logged and reviewed.

D privilege : is allocated only to Gary Powell the IT manager. This is a very seldom used privilege and is used to delete a record from the masterfile under valid circumstances, e.g. a debtor who is no longer a customer. To delete any record from a masterfile requires firstly that the balance on the account be nil and a balance can only be reduced to nil by a transaction which would normally reduce that balance, e.g. in the case of a debtors balance, a payment received from the debtor, a credit note or journal entry. The record could then be deleted but the deletion would be logged.

C privilege : this is allocated to those people who need "change" access to perform their functions, and it is usually restricted to certain fields only. For example a debtor may wish to change their postal address; with her C privilege, the debtors clerk, Amy Mostert could change this address (but not other fields pertaining to the debtor) from her terminal.

I privilege : this is allocated to most people in a particular cycle and it allows them to obtain information from the masterfile, necessary to do their jobs. For example, a clerk taking an order over the telephone may want to check inventory availability or the credit standing of the customer. The "I" privilege enables him or her to get the information required. Obviously he or she cannot "add" "delete" or "change" any information; effectively read only access has been granted.

On accessing the relevant application, if the user has any masterfile privileges, the masterfile amendment module menu will appear on screen but the employee will only be able to select the privileges linked to his user ID, password and user profile e.g. change an address or add a new employee (this is the identification, authentication and authorisation process in action).

It is interesting to note that at ProRide (Pty) Ltd, neither the financial director, nor the managing director have anything other than "I" privileges. This is because the managing director does not require other privileges and the financial director is an important part of the (independent) approval process for important amendments. (The financial director does have the "release" privilege for EFT payments.)

7. UPDATING THE GENERAL LEDGER

As explained in 3.1 above, the general ledger software is resident on the AS 400 whilst the software for a number of other cycles is not. This means that to keep the general ledger up to date it is necessary to pass a series of journal entries at month end. These journal entries are entered by Johan Els (financial manager) from his PC. Access to the "journal entry module" is restricted to Johan using the normal access control techniques. A listing of all journal entries is produced and checked to source the following day by Dalene Burger, the accounting supervisor.

CHAPTER 10

REVENUE AND RECEIPTS CYCLE

CONTENTS

		Page
ACCOUNTING SYSTEM AND CONTROL ACTIVITIES		10/2
1.	Introduction	10/2
2.	Characteristics of the cycle	10/2
3.	Objective of the first section of the chapter	10/2
4.	Basic functions for any revenue and receipts cycle	10/2
5.	Narrative description of a manual revenue and receipts cycle by function	10/3
6.	Documents in the cycle	10/6
7.	Flow charts for a manual revenue and receipts cycle	10/7
8.	Computerisation of the revenue and receipts cycle	10/20
9.	Internal control in a cash sales system	10/40
10.	The role of the other components of internal control in the revenue and receipts cycle	10/42
NARRATIVE DESCRIPTION OF THE CYCLE AT PRORIDE (PTY) LTD		10/44
AUDITING THE CYCLE		10/54
1.	Introduction	10/54
2.	Financial statement assertions and the revenue and receipts cycle	10/54
3.	Important accounting aspects	10/55
4.	Fraud in the cycle	10/55
5.	Further audit procedures	10/56
6.	Tests of controls	10/57
7.	Substantive procedures	10/59
8.	Substantive testing of sales	10/61
9.	Substantive procedures for the audit of trade receivables	10/63
10.	The use of audit software (substantive procedures)	10/66
11.	Other audit procedures	10/69
12.	Substantive procedures for the audit of bank and cash	10/70

ACCOUNTING SYSTEM AND CONTROL ACTIVITIES

1. INTRODUCTION

The revenue and receipts cycle is sometimes referred to as the sales and collection cycle and perhaps this name better describes the activities of the cycle. This chapter deals initially with the accounting system (which is part of the company's information system) and the control activities which are put in place to control the sale of the company's goods or services, and the collection of amounts owed in respect of those sales. The latter part of the chapter deals with the audit of the cycle.

2. CHARACTERISTICS OF THE CYCLE

2.1 Variation.

There are any number of different products and services which are sold by companies, which means that there will be plenty of variations in the systems you encounter in practice. For example, goods can be sold over the counter, over the internet, over the phone or as a result of a hardcopy customer order. Physical objects are sold as well as non-physical objects (e.g. services) and a "sale" may take a long time to complete (e.g. in a construction contract) or may be instantaneous, (e.g. over the counter cash sale).

2.2 Cash sales.

Many businesses sell goods for cash and on credit to account holders. Having cash in the business is a security risk which must be addressed. There is a potential for theft and physical harm to employees who deal with cash.

2.3 Credit sales.

When a company allows a customer to charge a sale made to an account (rather than settle the amount immediately by say, cash, credit card or cheque), there is a risk that the customer will not pay, and the company will suffer a loss. Important activities in a revenue and receipts cycle will be the checking of creditworthiness of a customer ***before*** the sale is made, and the timeous collection of amounts owed.

2.4 Legislation.

For companies who sell to consumers, e.g. retailers, the Consumer Protection Act is an important act which must be complied with.

3. OBJECTIVE OF THE FIRST SECTION OF THE CHAPTER

Our objective in the first section of this chapter is to provide you with the necessary information to understand how revenue and receipts cycles function. As discussed in paragraph 2, revenue and receipts systems can vary considerably; the approach in this chapter is to provide a thorough knowledge of a manual system and then to illustrate how things may change as computerization is introduced into the system. Remember that computerization does not change what is required of the system, e.g. take an order, pick the goods, raise an invoice etc, but it does change how the transactions are carried out and recorded.

4. BASIC FUNCTIONS FOR ANY REVENUE AND RECEIPTS CYCLE

For the purposes of this text, we have chosen to describe a system for a business which has conventional functions; it receives orders from its customers, supplies the goods from its warehouse and charges the sale to the customer's account. These functions which are essentially those required for most revenue and receipts cycles can be broken down as follows:

4.1 Order department

* ***receiving customer orders*** : these may be received in a variety of ways, e.g. by phone, receipt of a customer's written order, over the Internet or over the counter
* ***authorising the sale*** : this will involve granting or confirming credit before the order is processed. This is an important activity because companies do not want to make sales for

which they will not be paid! (At the authorising stage, an inventory availability test may also be carried out to confirm that the order can be filled).

4.2 Warehouse/despatch

* ***processing the order*** : this involves the manual process of gathering together (picking) the goods from the stores to fill the order
* ***despatch*** : this is the manual process of releasing the goods ordered to the customer. The customer may collect the goods, the goods may be delivered by the company's own delivery vehicle or by a transport company, e.g. railways, courier service.

4.3 Invoicing

* this is the very important step of notifying the customer of the amounts owed for goods purchased. The invoice may be sent with the goods, or at a later stage. There is no fixed rule, but generally the sooner the invoice is sent, the sooner the customer pays.

4.4 Recording sales and raising the debtor

* this involves creating the records of the sales that have been made, as well as who owes the company money, i.e. debtors.

4.5 Receiving and recording payment from debtors

* this is also a very important step and involves collecting payment from debtors, ensuring payment is banked and recording the receipts in the cash receipts journals and debtor's ledger.

4.6 Credit management

* ***evaluating creditworthiness:*** these are the activities carried out to determine whether credit can be extended to a customer, and if so, what the terms (how long the debtor is given to pay, e.g. 60 days) and limits (the amount of credit, e.g. R20 000) will be
* approving sales orders particularly those which are from debtors who have exceeded their credit terms and/or limits
* ***collecting amounts owed***: these are the activities carried out to ensure amounts owed by debtors, are paid when they are due.

In addition to the above, there are other lesser activities within the cycle which must be controlled. They are

* controlling goods sold but which have been returned by the customer
* passing credit notes for goods returned or other reasons e.g. overpayment by a debtor
* granting discounts on payments from customers
* considering and effecting write offs of bad debts.

5. A NARRATIVE DESCRIPTION OF A MANUAL REVENUE AND RECEIPTS CYCLE BY FUNCTION

5.1 Order department

* as the name suggests, the order department is responsible for receiving orders from customers and setting in motion the filling of the order. This will involve instructing the warehouse department to select the items ordered from the stores so that the items can be despatched to, or picked up by, the customer. Before setting this process in motion, the order department should confirm that the customer's account is "up to date" i.e. the amount owed is within the terms and limit set for that customer and that processing the current order will not push the customer beyond his credit limit.

  Example. Stepps (Pty) Ltd, a customer of Ladderland Ltd, has a credit limit of R50 000 on its account and must pay within 60 days. If an order for goods costing R10 000 is received, the order department must check whether any portion of the balance on Stepps (Pty) Ltd's account has been outstanding for longer than 60 days and that the current balance is no more than R40 000. If Stepps (Pty) Ltd is not within its terms and limit, the order department will need to obtain the authorisation of the credit management department to initiate the sale. In most businesses, the order department will also confirm that the goods ordered by the customer are "in stock" (available) before initiating the sale. If goods are not "in stock", the sales order

clerk will contact the customer to ask whether the customer wishes the order to be placed on a back order list to await the arrival of more inventory.

* in a manual system, all orders received by the order department should be entered manually onto a pre-printed, sequenced, multicopy, internal sales order (ISO) regardless of how the order is received, e.g. by phone, through the post, fax or by email
* the order clerk will take the ISO to the credit management department to have the ISO signed (authorised) once the customer's credit standing has been checked by that department
* if an order is received from a non-account holder, the credit management department will go through the process of checking the customer's creditworthiness and setting credit terms and limits as described in 5.6
* a copy of the ISO will be delivered to the warehouse to act as the "picking slip" i.e. the document which informs the warehouse employees as to which goods to select for despatch to the customer
* a copy of the ISO will be filed in the order department in numerical sequence and a copy will be sent to the accounting department.

5.2 Warehouse/despatch

* the warehouse/despatch function is required to select the goods to be sent to the customer in terms of the ISO/picking slip. (In multipart stationery, the second copy of the ISO can be headed "picking slip"). This function will also be responsible for controlling the removal of the goods from the warehouse to the despatch area for delivery to, or collection by, the customer (i.e. the goods should be signed out of the custody section of the warehouse and into the despatch section).
* in a manual system, the ISO/picking slip sent to the warehouse will be given to a warehouse employee to select (pick) the goods listed on the ISO/picking slip
* this employee will tick off the goods picked on the picking slip and mark clearly any items which are not available (note: inventory availability checks carried out in the order department are not foolproof and some companies may choose to make out the ISO without carrying out the inventory availability test. Using this method, "out of stock" items will be identified at the "picking" stage.)
* a warehouse clerk will then manually complete a pre-printed, multi-part, sequenced delivery note, detailing the goods picked
* once the delivery note has been completed, the goods will be moved to the despatch area with the supporting documentation where they will be checked, boxed or packaged. The despatch clerk will sign the documentation (copy of the delivery note or picking slip) to acknowledge the transfer of the goods into his custody
* when the goods are despatched to the customer they will be accompanied by two copies of the delivery note, both copies will be signed by the customer, one of which will be retained by the customer and the other returned to the company
* where goods are to be delivered to the customer (not collected), delivery lists will be compiled and the goods loaded onto the delivery vehicle under supervision. The driver will acknowledge taking custody of the goods by signing the delivery list.

5.3 Invoicing

* the objective of invoicing is to notify the customer promptly of the amount due
* accounting employees will collect together the supporting documentation for the sale which has been made, e.g. the ISO, and the copy of the delivery note signed by the customer. They will check all the details of the sale and create an invoice
* a copy of the invoice will be sent to the customer. (Note: in some systems the invoice is made out at the same time as the delivery note. This may lead to more errors in invoicing because the invoice is made out ***before*** the customer has checked and accepted the goods, but does have the advantage of getting the invoice to the customer sooner.)
* a pre-printed, multi-copy, sequenced invoice will be made out manually, taking the details from the supporting documentation
* debtor details, pricing, discounts, casts and extentions and VAT will be checked, and a copy of the invoice sent to the customer.

5.4 Recording of sales and raising debtors

* the purpose of this function is to create a record of sales (the sales journal) and to raise the amount owed by the customer as a debtor (debtors ledger).
* in a manual system, a copy of each of the invoices for the period (day, week, month) will be sent to the designated accounting clerk who will write up the invoices in the sales journal in numerical sequence
* before the total of sales is posted (transferred) to the general ledger and the individual sales are posted (transferred) to the debtors ledger, another staff member will check the sequence of invoices entered in the sales journal, follow up on any missing numbers, and check the accuracy of the amounts entered in the sales journal against the invoices themselves
* amounts will then be posted (transferred) to the respective ledgers.

5.5 Receiving and recording payments from debtors

* the objective of this function is to accurately record the receipts of payments from a debtor. The function will include the "mailroom" (mail receiving function)
* a business receives a lot of important mail through the postal system. This may include purchase orders from customers, invoices and statements from suppliers, notifications, requests, etc from SARS and other regulatory bodies as well as cheques (or postal orders or even cash!) from debtors
* there are basically three ways in which debtors pay, i.e. by cash, cheque or by direct deposit into the company's bank account. This can be done by the debtor going to the company's bank and depositing cash or a cheque directly into this bank account or by effecting an electronic funds transfer (a transfer from the debtor's bank account to the company's bank account)
* it is very seldom that a company will pay another company by cash, and payment by cheque is becoming far less common. However, payments by cash or cheque are still carried out and the accounting system must accommodate these methods of payment
* direct payments into a company's bank account are quicker and safer but do change the procedures and control activities for receiving and recording payments from debtors
* at the end of the month, the debtors clerk will draw up a statement for each debtor which summarises the transactions with that customer for the month, e.g. sales made, payments received, credit notes issued. The balance on the statement which will be sent to the customer should reconcile with the debtors' account in the debtors ledger
* all incoming mail of business importance will be recorded in a remittance register and distributed to the relevant department. This will be a "physical" activity
* receipts will be made out manually for all payments received by the employees opening the mail. Cash and cheques, after being receipted and recorded in the remittance register, will be sent to the cashier
* the cashier will agree the cash and cheques received, to the remittance register and receipts and make out a bank deposit slip
* cheques and cash will need to be (physically) taken to the bank to be deposited
* the other part of this function is to record the receipts from debtors in the cash receipts journal. The cash book clerk will write up the cash receipts journal from the receipts and deposit slips and will subsequently post (transfer) the amounts to the debtors ledger and general ledger
* where a debtor has paid directly into the company's bank account, the debtors clerk will need to obtain a bank statement from the bank. This will reflect the payments made directly into the company's bank account. A schedule of these receipts will be drawn up and used to write up the cash receipts journal.

5.6 Credit management

* the main objective of this function is to minimise the risk of losses from bad debts. The control activities centre around extending credit only to creditworthy customers, setting reasonable credit terms and limits, preventing customers from exceeding their limits, and following up promptly on debtors who are showing signs of falling behind in their payments. The passing of credit notes may also be managed by this function.
* in a manual system, all documentation will be hardcopy and follow up of information supplied by a prospective customer in the credit application form, will be followed up by a phone call or letter. The credit limits and terms will need to be recorded on a schedule or in the debtors ledger. Authorisation of a customer order (ISO) will be a manual exercise.

6. DOCUMENTS USED IN THE CYCLE

6.1 Customer order.

The customer's instruction as to what goods are required (could be sent by post, email, fax or orders could also be placed over the phone)

6.2 Internal sales order.

A document compiled by the company's own sales order clerk which records the goods ordered by the customer. It is used for sales authorisation and as a basis for creating the picking slip. A very important document where orders are taken orally e.g. over the phone

6.3 Picking slip.

This document lists all the items which the customer has ordered. It is used to assist the stores personnel to "pick" the goods needed to fill the order from the store so that they can be despatched to the customer

6.4 Invoice.

The document which is sent to the customer to notify them of the quantity and price of the goods sold to them, the total amount of the sale, discounts and VAT

6.5 Delivery note.

This document details the date, description and quantity of the goods despatched to the customer and is signed by the customer to acknowledge receipt of the goods. When the company delivers to its customers, details of the deliveries e.g. address, delivery note number, will be entered on a ***delivery list*** which is used by the delivery staff to schedule and control deliveries

6.6 Statement.

A summary of all of the transactions for a period, usually a month, sent by the company to the customer. The statement reflects the opening balance, sales made, payments received, other adjustments such as credit notes, and the closing balance as well as a breakdown of the periods for which the total amount owed has been outstanding e.g. 30 days, 60 days, 90 days and over

6.7 Credit application form.

This document is filled in by a prospective customer so that the customer's credit worthiness (ability to pay) can be evaluated. The customer will be required to provide trade references, income and expenditure details, bankers etc., which are then followed up by the company. Trade references and credit bureaux are usually contacted before the company decides on a credit limit and terms appropriate for the customer

6.8 Receipt.

The receipt records details of payments received from customers

6.9 Remittance advice.

A document sent by the customer with their payment to indicate precisely which invoices are being paid. Where a payment is made directly into the company's bank account by direct deposit or EFT, the customer should send the remittance advice (and proof of payment) under separate cover

6.10 Remittance register.

A register or list of payments received by the company. (Payments from debtors not deposited directly in the company's bank account by the debtor.)

6.11 Credit note.

A document which is made out by the company and sent to the customer to acknowledge that the customer's account has been reduced (credited) for some reason other than for a ***payment*** received, e.g. goods have been returned by the customer for which credit must be passed

6.12 Deposit slip.

This is a bank document which is filled in by the company to record the deposit of payments received from the customer, into the bank

6.13 Price lists.
Document containing prices (and discounts) of the company's products to be referred to by the sales order clerk when customers require prices on placing orders

6.14 Back-order note.
A document which contains details of goods which could not be supplied when ordered by a customer as there was no inventory available. The back order notes are filed and regularly and frequently reviewed to establish whether an order has been placed with a supplier for the outstanding goods

6.15 Goods returned voucher.
A document made out by the company itself, which is used to record the details of goods which have been returned by a customer

6.16 Masterfile amendment form (computerised system).
A document used to record an amendment to the debtors masterfile

6.17 Logs, variance reports, etc
In a computerised system, the computer can be programmed to compile logs, variance reports, etc. A log is simply a record of an activity which has taken place on the computer, e.g. a log of masterfile amendments.

In addition to the above documents, the company will make use of a sales journal, cash receipts journal (cash book), a sales returns and allowances journal (into which details of credit notes etc. will be entered) and the debtor's ledger. In a computerised system there will be transaction files and the debtors masterfile. Documents used in the system will essentially be the same, but will be printed off the computer where necessary.

7. FLOW CHARTS FOR A MANUAL REVENUE AND RECEIPTS CYCLE

A flowchart of the cycle is presented on the following two pages. The intention of these flowcharts is to keep them simple so that you can get a basic understanding of what happens in the cycle. This is followed by a series of tables which expand on the functions, risks and control activities in the cycle.
We have chosen to illustrate the cycle as a manual accounting system as it is very important for you to understand the basics. Once you have mastered the basics, it is considerably easier to understand the introduction of computerisation into the cycle.

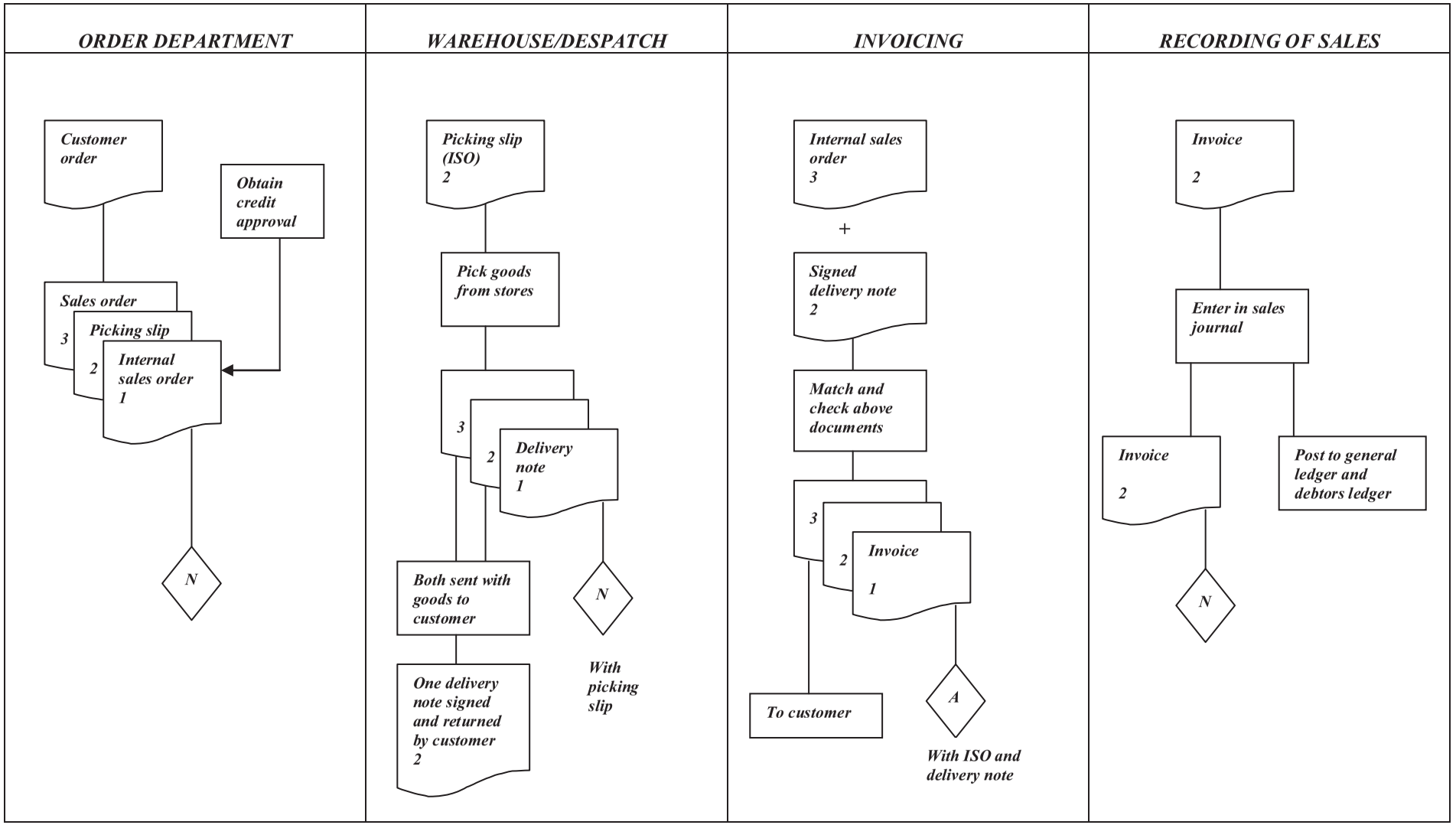
7.1 The functions which are described in the tables and/or flowchart are

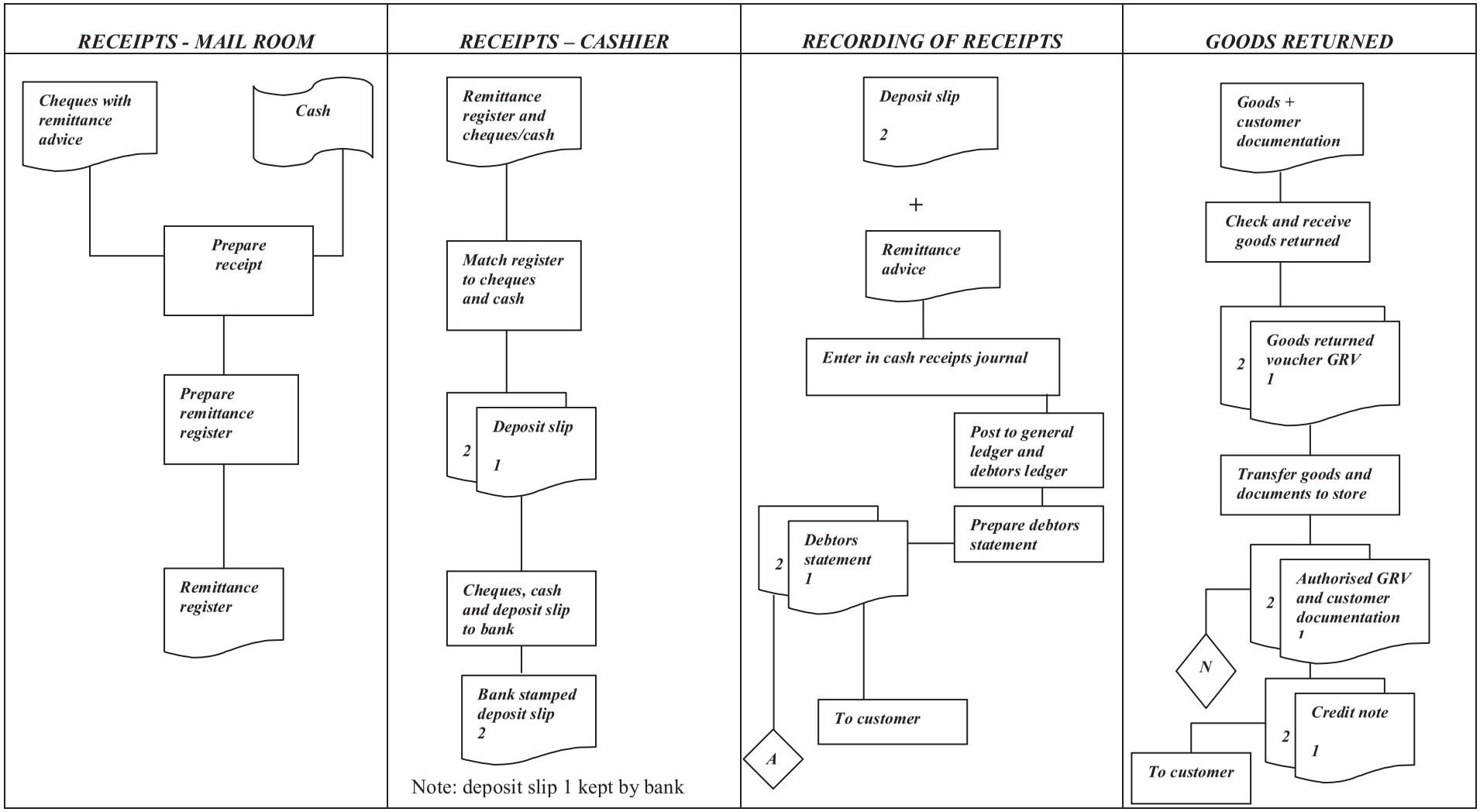
Order department
* receiving customer orders
* sales authorisation

warehouse/despatch
invoicing
recording of sales/debtors
receipts of payments from debtors
recording of receipts
goods returned by customers
credit management

7.2 For the purposes of the illustration, we have chosen a reasonably straight forward company with the following characteristics
* adequate staff for sound division of duties
* phone orders and documented orders are accepted
* credit sales only, although some debtors send cash in the post to pay their accounts (for illustration purposes!)
* receipts are made out for all payments from debtors
* no inventory availability test is conducted when orders are received; "out of stock" items are identified at the "picking" stage
* the company makes all of its own deliveries to customers
* there is a sound control environment and the appropriate properly designed documents and records e.g. ledgers and journals, are used.

We suggest you use the flow charts in conjunction with the narrative description (para 5) and the schedules on pages 10/10 to 10/19.


ORDER DEPARTMENT
WAREHOUSE/DESPATCH
INVOICING
RECORDING OF SALES
Customer order
Obtain credit approval
Sales order
3
Picking slip
2
Internal sales order
1
N
Picking slip (ISO)
2
Pick goods from stores
3
2
Delivery note
1
Both sent with goods to customer
One delivery note signed and returned by customer
2
N
With picking slip
Internal sales order
3
+
Signed delivery note
2
Match and check above documents
3
2
Invoice
1
To customer
A
With ISO and delivery note
Invoice
2
Enter in sales journal
Invoice
2
Post to general ledger and debtors ledger
N
KEY
N
= Filed numerically,
A
= Filed alphabetically,
= document
= action


RECEIPTS - MAIL ROOM
Cheques with remittance advice
Cash
Prepare receipt
Prepare remittance register
Remittance register
RECEIPTS – CASHIER
Remittance register and cheques/cash
Match register to cheques and cash
2
Deposit slip
1
Cheques, cash and deposit slip to bank
Bank stamped deposit slip
2
Note: deposit slip 1 kept by bank
RECORDING OF RECEIPTS
Deposit slip
2
+
Remittance advice
Enter in cash receipts journal
Post to general ledger and debtors ledger
Prepare debtors statement
2
Debtors statement
1
To customer
A
GOODS RETURNED
Goods + customer documentation
Check and receive goods returned
2
Goods returned voucher GRV
1
Transfer goods and documents to store
2
Authorised GRV and customer documentation
1
N
2
Credit note
1
To customer

RECEIVING CUSTOMER ORDERS (ORDER DEPARTMENT)		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
To record orders from customers and initiate action to fill them. Orders will be received in document form (customer order) or over the telephone. Internet orders are dealt with in Chapter 9. Persons receiving the order need to establish that the customer is a valid customer and that the details of the order are accurate and complete in every respect, e.g. description, quantity, delivery address. As this is the initiation of the transaction, it is particularly important to get everything right. If customer does not have an account they must be referred to the credit manager who will send the customer a credit application.	Customer order Internal sales order (ISO) Price lists	* order may be accepted from a non-account holder. * orders may not be acted upon timeously or at all, resulting in a loss of sales and customer goodwill. * inaccurate or incomplete order details may be recorded which will result in incorrect deliveries, returns and customer dissatisfaction.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. record ***all*** orders on sequentially numbered internal sales orders. 2. no orders to be accepted if the customer is not an approved customer, e.g. no account number (NB we are dealing with a credit sales system). Order clerk will check approved customer list 3. attach customer order to internal sales order and have second staff member cross check detail (if practical) 4. for phone orders, order clerk to: 4.1 request customer's account number 4.2 request customer's order reference 4.3 confirm all order details, including delivery address and price of goods, by reading order details recorded back to customer 5. order clerk to sign all ISOs to indicate performance of control activities 6. on a regular basis, ISOs to be sequence checked (for completeness), and matched to delivery notes to identify any orders that have not been acted upon. Note: If necessary, order clerk should have price lists, lists of customer account numbers, and inventory descriptions and codes to check validity and accuracy of information supplied by customer. (This is very easy in a computerised system.) Note: employees must sign documentation/records to acknowledge the control procedures they have conducted Note: these controls are essentially ***preventive*** in nature Note: many companies which take orders over the phone, will supply customers with product catalogues which include descriptions and product codes.

SALES AUTHORISATION (ORDER DEPARTMENT)		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
To assess whether orders should be accepted. The intention is to determine whether the customer is creditworthy and has not exceeded his credit limit. The function begins earlier when the customer completes a credit application form which is evaluated and credit limits and terms are set. (see "credit management" on 10/19)	Credit application and debtors ledger	* A sale will be made to a customer who is not creditworthy i.e. will not pay, resulting in a loss to the company.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. before processing the order, checks should be carried out by the credit controller (department) to establish: 1.1 that the customer has not supplied fictitious details 1.2 customer's credit status is satisfactory by reference to the customer's details, e.g. his account balance and credit terms held on file and/or in the debtors ledger 2. ISOs (picking slip) to be authorised by signature of the credit controller before being sent to the warehouse Where the order is from a prospective customer, credit application procedures must be conducted before the order is filled: * the credit application form must request the customer to provide banking details, trade references, income and expenditure details * the credit controller must follow up by contacting trade references and credit bureaux and assessing customer liquidity * terms and limits must be set by the credit controller and approved by the financial manager. Note: employees must sign documentation/records to acknowledge the control procedures they have conducted and the financial manager must not approve the terms and limits without reviewing the supporting documentation.

WAREHOUSE		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
To fill accepted orders promptly and accurately and to ensure only authorised orders are acted upon. This is the manual function of picking the goods from the warehouse using a signed copy of the ISO (picking slip), and creating a delivery note. Goods which cannot be picked because they are ″out of stock″ will also be identified and a back order note created.	Picking slip Delivery note Back order note	* valid ISO/picking slips may not be acted upon. * goods may be removed (picked) from inventory for fictitious/unauthorised sales. * incorrect items and quantities may be picked. * inaccurate and incomplete delivery notes may be made out. * "out of stock" items may not be identified on the picking slip. * customer not notified of "out of stock" items resulting in loss of the sale and customer goodwill.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. picker to initial the picking slip for each item picked and identify on the picking slip, items which cannot be supplied (out of stock) 2. supervisory checks should be carried out by the warehouse foreman to ensure that all goods picked are supported by signed picking slips. See also control activity number 1 under "despatch". 3. warehouse clerk to 3.1 check goods picked to picking slip 3.2 prepare delivery note from picking slip (delivery note cross-referenced to picking slip) 3.3 prepare back order note from the picking slip and cross reference both documents (see also control activity number 1 under "despatch") 3.4 send copy of the back order note to order clerk to enable the order clerk to notify customer 3.5 send copy of the back order note to the buying department 4. order clerk to follow up back orders regularly and frequently. When inventory becomes available, order clerk should confirm that the customer still requires the goods and, if so, make out an ISO to initiate the sales process. (The back order note in effect becomes the customer order) 5. delivery notes and picking slips to be matched and filed numerically. Unmatched picking slips to be followed up to determine whether goods have been picked. Note: employees must sign documentation/records to acknowledge the control procedures they have conducted.

DESPATCH		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
To ensure that only goods supported by properly authorised picking slips, and accompanied by accurate and complete delivery notes, are despatched. To ensure prompt despatch of goods which have been picked, to the correct customer. Once the goods have been picked and delivery notes made out, they are transferred to despatch to be packed, labelled and delivered. Controls must be sound because, by this stage, the goods have left the custody of the warehouse and are thus susceptible to theft. In addition, the goods are moving between a number of parties, so isolation of responsibility is very important.	Delivery note List of deliveries	* theft may be facilitated by uncontrolled despatch. * despatch errors may occur • incorrect goods or quantities despatched • goods delivered to wrong customer * customers may deny having received goods. * goods released from the warehouse are never despatched.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. on receipt of the goods, picking slip and delivery notes from the warehouse, the despatch clerk should 1.1 check quantities and description of goods against the authorised picking slip and delivery note 1.2 sign picking slip and delivery note to acknowledge receipt of goods 1.3 retain two copies of the delivery note and return the signed picking slips to the warehouse (once goods are packed) 2. the goods picked should be checked to the picking slip and delivery note as they are packed into a box for delivery. The address on the box should be checked against the delivery address on the documentation and the box sealed immediately 3. despatch clerk should prepare a two part list of deliveries to be made. The list should be matched to the delivery notes and the physical goods loaded onto the vehicle e.g. delivery note P1234 – 4 boxes 4. delivery staff (e.g. driver) should supervise loading the truck and sign a copy of the delivery list to acknowledge receipt of the delivery notes and the corresponding goods • driver to retain one copy of delivery list, and the delivery notes • despatch clerk to retain signed copy of delivery list 5. gate controls e.g. security, should check all goods to be delivered appear on the delivery list and are supported by delivery notes. Both copies of each delivery note should be date stamped by gate control (gate controls can be impractical – if they are, then despatch controls must be very tight) 6. on delivery, the customer should sign both copies of the delivery note (having checked the goods), retain one copy and return the other copy with the driver Note: employees must sign documentation/records to acknowledge the control procedures they have conducted.

INVOICING		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
To notify the customer promptly of amounts due for goods supplied. On return of the signed delivery note from the customer it should be matched with the sales order and an invoice should be generated.	Sales invoice Price lists	* goods despatched may not be invoiced. * invoices may be inaccurately prepared/misstated (prices, quantities, descriptions, discounts, VAT)

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS

1. a copy of the internal sales order should be held in numerical order in a temporary file in the "invoicing section" (accounting department)

2. as signed delivery notes are received they should be matched to their ISO and filed sequentially by delivery note number.

3. on a frequent and regular basis, ISOs remaining on the temporary file should be investigated

4. the file of matched delivery notes should be sequence tested and gaps in sequence investigated

5. the invoice clerk should:
   - 5.1 compare details on the ISO and delivery note
   - 5.2 check prices quoted to the customer, and entered on the ISO, against official price lists and discount schedules
   - 5.3 prepare a numerically sequenced invoice and cross reference it to the delivery note/customer order

6. second employee (supervisor) to check and sign invoice after checking :
   - 6.1 prices, extentions, casts
   - 6.2 discount and VAT calculations
   - 6.3 customer details

Note: employees must sign documentation/records to acknowledge the control procedures they have conducted.

RECORDING OF SALES		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The purpose of this function is to record the sales made and to raise the corresponding debtor promptly. Invoices must be recorded accurately and entered against the correct debtor in the debtors ledger. Total sales for the period must also be posted to the sales and debtors control accounts in the general ledger.	Invoice Sales journal Debtors ledger General ledger	* invoices are omitted from the sales journal * invoices are duplicated in the sales journal * invoices are inaccurately entered in the sales journal e.g. R4325.50 entered as R432.55 * invoice entered against incorrect debtor when posting (transferring) to the debtors ledger accounts.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. invoices to be entered in the sales journal in numerical sequence 1.1 sequence to be continued period to period 1.2 the numbers of any cancelled invoices to be recorded in the sales journal and marked "cancelled" 2. prior to entry in the sales journal, invoices to be added to obtain control total. This control total is then compared to the total in the sales journal after entry of individual invoices (batch control system). 3. independent staff member to: 3.1 sequence check sales journal entries and follow up on any missing invoices 3.2 compare customer name and amount entered in sales journal to the invoice for accuracy 3.3 check postings (transfers) from the sales journal to the debtors ledger (individual debtors) and general ledger 4. reconciliation of the debtors ledger to debtors control account in the general ledger on a regular basis, to be conducted by an independent employee. Note: employees must sign documentation/records to acknowledge the control procedures they have conducted.

RECEIPTS MAIL ROOM/CASHIER		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The arrival of a payment from a debtor is recorded and prepared for banking. Receipts should be made out for all cash received and possibly for cheque payments as well.	Remittance register Customer remittance advice Receipts Bank deposit slip	* payments received may not be banked due to theft or carelessness.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. post must be opened by two people working together 2. all payments received in the post should be recorded in a remittance register by those responsible for opening the post and a receipt should be made out for each payment received 3. prenumbered receipts should be issued for all payments received 4. all amounts received should be banked daily 5. deposit slip to be made out by the cashier, not the employees opening the post 6. cashier to reconcile cheques and cash to remittance register and receipts before accepting them for banking (remittance register should be signed by the cashier to acknowledge acceptance of the cash and cheques) 7. the remittance register and receipts issued should subsequently be reconciled to bank deposits (bank statement) by an independent supervisory employee 8. bank deposits should be reviewed regularly and gaps in daily banking, investigated by management Note: employees must sign documentation/records to acknowledge the control procedures they have conducted Note: payments by debtors are most frequently made directly into the company's bank account either by direct deposit (customer going to the bank and depositing the amount owed) or by electronic funds transfer (a transfer directly from the debtors' bank account to the company's bank account). To control this, the debtors clerk should obtain (download) bank statements frequently from the bank and compile a list of payments from debtors. Where possible, this list should be matched to remittance advices "proof of payment" documents, sent by the customer. The list should be checked by a supervisory level employee and used to write up the cash receipts journal. The list should be compiled on preprinted, sequenced documents and filed in numerical order (which should also be in date order).

RECORDING OF RECEIPTS		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The role of this function is to record the receipts from debtors in the cash receipts journal and credit the debtors' accounts promptly. Receipts must be recorded accurately and entered against the correct debtor. The total amount received from debtors for the period must also be posted to the debtors control account in the general ledger.	Bank deposit slip Cash receipts Journal (CRJ) Debtors ledger General ledger	* deposits may never be recorded/not recorded timeously. * recorded deposits may be : • inaccurate (errors) • overstated (fictitious deposits) • credited to the wrong debtor

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. the cash receipts journal should be written up on a daily basis by date and receipt number (if receipts are issued) 2. supervisory staff should review cash receipts journal for missing dates and gaps in sequence of receipts. They should also test postings to the debtors ledger 3. the "cash book" should be reconciled to the bank statement every month by an employee independent of the banking/recording of cash. The bank reconciliation should be reviewed by a senior (financial) employee 4. queries from debtors should be investigated by an employee independent of debtors and banking 5. reconciliation of the debtors ledger to the debtors control account in the general ledger should be conducted on a regular basis by the financial accountant Note: employees must sign documentation/records to acknowledge the control procedures they have conducted.

GOODS RETURNED BY CUSTOMER		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The role of this function is to control goods that have been returned by customers. The goods must be recorded on their return and the debtor's account must be credited. This requires the creation of two documents, a goods returned voucher, and a credit note. Credit notes will be recorded in a returns and allowances journal. Particular attention must be given to the control of credit notes.	Goods returned vouchers Credit note Returns and allowances journal Debtors ledger General ledger	* the description and quantity of goods returned may be incorrect resulting in an incorrect credit note being passed. * a credit note may be passed for goods which have not been returned. * credit notes may be inaccurately recorded and credited to the incorrect debtor.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS

1. all goods returned must be received by the company's goods receiving department

2. the goods receiving clerk must:
   2.1 count and check the description of the goods being returned (check also for damage)
   2.2 make out a goods returned voucher, cross referencing it to customer documentation
   2.3 sign and retain a copy of the customer documentation and attach it to the goods returned voucher

3. on transfer of goods from receiving into the warehouse, the stores clerk must:
   3.1 check description and quantity of physical goods to goods returned voucher and customer documentation
   3.2 sign to acknowledge the transfer of the goods into his custody

4. credit notes to be:
   4.1 made out by accounting department
   4.2 cross referenced to original invoice
   4.3 presented to a supervisory employee (with signed goods returned note and customer documentation). This staff member must be satisfied that granting of the credit note is valid and that the company's policies have been adhered to e.g. the goods cannot be returned, say, after 30 days from purchase date

5. credit notes to be entered sequentially in returns and allowances journal and normal control procedures over recording to be put in place

6. senior (financial) manager should review this journal frequently and follow up on suspicious credit notes, e.g. large amounts, credit notes to the same customer on a regular basis

Note: care must be taken to identify goods returned which are defective/damaged as these should not be returned to the inventory of saleable items. Defective/damaged goods will be received from the customer in the manner described (this facilitates the credit note) but must be carefully identified as damaged/defective.

Note: employees must sign documentation/records to acknowledge the control procedures they have conducted

CREDIT MANAGEMENT		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The purpose of this function is to limit the loss from bad debts and to encourage debtors to pay promptly. The function is closely linked to sales authorisation and as explained under that function, the process begins with sound controls over the acceptance of new customers and the extent of credit granted to them. Credit management should also identify debtors to be handed over to lawyers and subsequently written off if necessary.	All records in the cycle are relevant Monthly statements Age analysis Credit bureau information	* debtors do not pay at all or pay late * debtors are prematurely or inappropriately written off * debts are written off without authority.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. credit application controls as discussed under sales authorisation (page 10/11) 2. monthly statements should be sent promptly to debtors by the debtors section (accounting dept) 3. monthly age analysis of debtors and immediate follow up by phone or letter if credit terms are exceeded 4. if this is not successful, the credit controller should personally contact the customer to (possibly) renegotiate credit terms or threaten the handing over of the debtor to a lawyer for collection 5. if still no success, the debtor must be handed over ***before*** too long a period has elapsed 6. if the debt cannot be recovered, the debt write off must be recommended by the credit controller and authorised by an independent senior financial employee after review of the supporting documentation 7. credit manager should reconcile all bad debt write offs after they have been entered in the journal to supporting documentation 8. senior (financial) manager should be provided regularly with sufficient information to effectively manage the debtors, inter alia, list of debtors over their limits and how they are being followed up, bank and debtors balances, the age analysis, list of debtors that have been written off. Note: employees must sign documentation/records to acknowledge the control procedures they have conducted.

8. COMPUTERISATION OF THE REVENUE AND RECEIPTS CYCLE

Before we deal with the computerisation of this cycle, it will be useful for you to remind yourself of the following points. You can also refer to chapter 8 for a more comprehensive discussion on these points.

8.1 Access.

Many businesses will run their accounting systems on a local area network. Simplistically speaking, this means that there will be a number of terminals, usually from different departments, "linked" together and sharing resources. So access to the network and to individual applications, must be carefully controlled;

* access to the network should only be possible through authorised terminals
* only employees who work in the various functions of the cycle need access to the revenue and receipts application and only to those modules or functions of the application necessary for them to do their jobs (least privilege/need to know basis). Certain managers will have read only access for supervisory and review purposes.

Various techniques are used to control access. For example, the user

* must ***identify*** himself to the system with a valid user ID
* must ***authenticate*** himself to the system with a valid password
* will only be given access to those programmes and data files to which he is ***authorised*** to have access in terms of his user profile.

Once the user has got onto the system, access is usually controlled by what appears or does not appear on the user's screen. For example, only the modules of the application to which the user has access will appear on the screen, or alternatively, all the modules will be listed, but the ones the user has access to will be highlighted in some way, e.g. a different colour. If the user selects a module to which he does not have access (this is determined by his user profile), nothing will happen and/or a message will appear on the screen which says something like "access denied". In another similar method of controlling access, the screen will not give the user the option to carry out a particular action. For example, certain sales orders awaiting approval from the credit controller are listed on a suspense file. Although other users may have access to this file for information purposes, when they access the file their screens will either not show an "approve" option, or the "approve" option will be shaded and will not react if the user "clicks" on it. Only the credit controller's screen will have an approve option which can be activated.

Remember that access controls are a very effective way of achieving sound segregation of duties and isolation of responsibilities.

8.2 Menus.

Current software is all menu driven and generally easy to use. Menus can be tailored to the specific needs of a user (based on the user profile) and "items" can be selected by a simple "click of the mouse". Menus facilitate access control and segregation of duties.

8.3 Integration.

The extent to which the accounting system is integrated will vary, but most systems these days are integrated in the sense that a transaction entered onto the system, will instantly update all the records it affects. For example, the processing of a sales invoice will simultaneously update the sales account, debtors masterfile, inventory masterfile and possibly the general ledger. This significantly improves the accuracy of the records ***but*** makes the control over input extremely important.

8.4 Screen aids and programme (automated) checks.

These control techniques which are obviously only available in computerized systems, help ensure that transactions processed actually occurred, were authorised and are accurately and completely recorded and processed. The extent to which these are incorporated into the revenue and receipts application will vary depending on the quality and cost of the software. These controls are essentially preventive at the input stage and detective thereafter.

8.5 Logs and reports.

A computer can be programmed to produce any number of logs and reports. These can be used as detective controls or for monitoring performance. For example, in the revenue and receipts system, a log of all debtors masterfile amendments should be produced by the computer. This log will be a listing of all amendments that were made, what the amendment was (e.g. credit limit changed) who made the amendment and when it was made. "Read only" access to this file will be given to a senior member of the revenue/accounting section so that the amendments made can be confirmed as being authorised, accurate and complete by reference to the masterfile amendment forms. This log can be printed out or accessed on screen. Another example in a revenue and receipts system would be the production of a report of all debtors who have exceeded their credit limits. This could be used to monitor the performance of the credit controller. The important point about logs and reports is that unless an employee actually uses them and follows up on any problems, they are worthless. Their huge potential value is that if the log and report files are properly access protected, they provide ***independent*** evidence of what has taken place on the computer. They form a very important part of the ***audit trail***.

8.6 Matching and minimum entry.

Once data is in the database other data can be "matched" against it. A simple example would be where a debtor's account number is matched against the debtors' masterfile to determine whether it is a valid number. The fact that data is stored in the database also means that the principle of minimum entry can apply. For example, when a customer wishes to place an order over the phone, the entry of a valid customer's account number will bring up all the other standing detail relating to the customer so that the sales person does not have to enter this data. The speed, accuracy and completeness of input is enhanced.

8.7 On system approval.

Where hardcopy documents require approval, it is usually just a matter of presenting the authorising employee with the document and supporting evidence. In a computerised system, approval is frequently given on the system itself and the supporting evidence is also frequently on the system as well. There will be variations on how this is done, depending on the software.

8.8 Audit trail.

An audit trail is a record of the activities which have happened on the system which enables the sequence of events for a transaction to be tracked and examined, from start to finish. It should be possible to identify a sale reflected in the general ledger and trace it back to the order received from the customer. A system where there is a poor audit trail, will be a weak system. The trail will often be a combination of electronic and hardcopy data.

A NARRATIVE DESCRIPTION OF A COMPUTERISED REVENUE AND RECEIPTS CYCLE

For the purposes of this illustration, we have described a sales system for a medium-sized wholesale company which sells its products (toys) to a large selection of retailers. The system has been simplified as the intention is to illustrate how control policies, procedures and techniques can be implemented. We have provided comments and explanations to clarify certain points as the intention is to convey principles and not the fine detail:

- Its accounting systems are integrated.
- Sales are made only on credit to approved customers.
- Sales transactions are entered and processed in real time and all records affected by the sale are updated instantly, e.g. debtors masterfile, inventory masterfile.
- Orders are taken from customers over the phone (obviously in practice, orders are also sent to the company via email, fax or post, but as the controls are essentially the same as for phone-in orders, we have not dealt with hardcopy or email orders). Telesales order clerks are located in their own secure area.
- The company is large enough to implement sound segregation of duties with separate departments, i.e. ordering, warehouse, etc.
- Debtors are invoiced at the time the goods are despatched.
- The company has a link to its bank and debtors are encouraged to pay by EFT.

The debtors masterfile
The debtors masterfile is central to the revenue and receipts system. Integrity of the masterfile must be maintained and access to the masterfile, particularly write access, i.e. the ability to make amendments, must be strictly controlled. Equally important is the control over the amendments themselves to ensure they are authorized (valid), accurate and complete. Unauthorised amendments could include adding a fictitious debtor (to record fictitious sales), changing (usually extending) credit terms or credit limits. With most modern accounting packages, trying to fraudulently reduce a debtors balance or delete the debtor would not be possible through the masterfile amendments module. To reduce a balance, a fraudulent credit note, journal entry or receipt would have to be processed. To delete the debtor altogether, the balance would need to be reduced to nil and then the delete process followed. This would be linked to a user profile and would be logged. Controls will be primarily preventive, but there will be detective controls. There will be both user and automated (programme) controls. Much of the information on the debtors masterfile is the responsibility of the credit management section, so it makes sense for this section to be primarily responsible for the integrity of the file and the amendments. All amendments should be logged and there must be independent reconciliation and review of the log by a senior employee, e.g. the financial manager.

Activity/procedure	*Control, comment and explanation*
1. Record all masterfile amendments on a source document.	1.1 ***All*** amendments to be recorded on hardcopy masterfile amendment forms MAFs (no verbal instructions) (see Note (b) on page 10/25). 1.2 MAFs to be pre-printed, sequenced and designed in terms of sound document design principles.
2. Authorise MAF.	2.1 The MAFs should be * signed by two reasonably senior employees in the section (e.g. credit controller and senior assistant) after they have agreed the details of the amendment to the supporting documentation, e.g. the approved credit application document for the addition of a new customer * cross referenced to the supporting documentation.

3. Enter only authorised masterfile amendments onto the system accurately and completely.	3.1 Restrict write access to the debtors masterfile to a specific member of the section by the use of user ID and passwords (see Note (a) on page 10/25). 3.2 All masterfile amendments should be automatically logged by the computer on ***sequenced*** logs and there should be ***no write access*** to the logs (this allows subsequent checking of the MAFs entered for authority) 3.3 To enhance the accuracy and completeness of the keying in of masterfile amendments and to ***detect invalid conditions***, screen aids and programme checks can be implemented. ***screen aids and related features*** * minimum keying in of information. For example when amending existing debtor records, the user will only key in the debtors account number to bring up all the details of the debtor * screen formatting, screen dialogue * the account number for a new debtor is generated by the system ***programme checks***, e.g. (see Note (c) on page 10/25) * verification/matching checks to validate a debtor account number against the debtors masterfile (invalid account number, no amendment) * alphanumeric checks * range and/or limit/data approval checks on terms and credit limit field, e.g. credit limit must be between R5 000 and R75 000 (range) or cannot exceed R75 000 (limit), and terms can only be 30 days or 60 days (data approval) * field size check and mandatory/missing data checks, e.g. credit limit and terms must be entered * sequence check on MAFs entered * dependency check e.g. the credit limit granted may depend upon the credit terms granted, e.g. a debtor granted payment terms of 90 days may only be granted credit up to a limit of R2 000 (a relatively low amount)

4. Review masterfile amendments to ensure they occurred, were authorised and were accurately and completely processed.	4.1 The logs should be reviewed regularly by a senior staff member e.g. financial manager 4.2 The sequence of the logs themselves should be checked (for any missing logs) 4.3 Each logged amendment should be checked to confirm that it is supported by a properly authorised MAF and 4.4 That the details, e.g. debtor account number, amounts, etc, are correct 4.5 The MAFs themselves should be sequence checked against the log to confirm that all MAFs were entered

Note (a): The authority needed to enter different types of masterfile amendment can be given to different levels of employee e.g. changing a credit limit may be restricted to a single senior employee, but changing an address or contact details could be assigned to a lower level employee.

Note (b): Unused MAFs and other important supporting documentation should be subject to stationery controls as it is more difficult to create an invalid masterfile amendment without the source document.

Note (c): A masterfile amendment should be carefully checked in all respects before it is authorised, e.g. the validity of credit terms and limits in relation to each other, so there should be a minimum of errors or invalid conditions having to be identified (detected) by the programme controls. Each company will decide for itself the extent of programme controls it wishes to implement.

Ordering

All orders from customers need to be entered into the system accurately and completely and subjected to creditworthiness and inventory availability checks.
Only orders from approved customers should be accepted. Remember that for the purposes of this illustration, orders are taken over the phone. A number of automated checks will be in place as the objective is to ***prevent*** errors in the information entered. The system will not allow the order clerk to continue taking the order if (programmed) automated checks are not satisfied. All employees in the cycle who make use of the computer to fulfil their functions will have user Ids and unique passwords and their screens will be "linked" to their user profiles. They will log onto the system in the normal manner.

Activity/procedure	***Control, comment and explanation***
1. Access the order system. We will assume that telesales operators (order clerks) each have their own terminal in a secure telesales area.	1.1 All incoming sales order calls are directed to a telesales order clerk (a queuing system will direct the call to the next available operator).

	1.2 Write access to the sales order module will be restricted to order clerks. 1.3 The order clerk's user profile gives him read only access to the debtors masterfile and the inventory masterfile. 1.4 As there is a dedicated telesales area, taking of orders may be restricted to terminals in this area (access controls are more commonly centred around users as opposed to terminals).
2. Identifying and authenticating the customer.	2.1 On receiving a phone call, the order clerk should request the customer's account number and key it in, a programmed (automated) verification check will take place. If it is a valid account number, the details of the customer will appear on the screen, e.g. name , delivery address, etc, formatted as a sales order. The computer has satisfactorily matched the account number against the masterfile. 2.2 The order clerk should then request the caller to provide other information which has appeared on the screen to authenticate the customer. Note, the order clerk should ***not*** give the information to the caller and ask him to confirm it – the caller must provide the information. 2.3 If the account number is a match to the debtors masterfile, the system will automatically allocate a ***unique transaction number*** which will identify the sales order as it progresses through the system. 2.4 If the customer does not have an account, he will not be on the debtors masterfile and will be referred to the credit management department. The system will not allow the order clerk to proceed with an order. 2.5 At the time the account number is validated against the debtors masterfile, the order clerk may receive a message on the screen that there is a "hold" on the account which prevents the order clerk from continuing with the taking of the order, e.g. the debtor may have been handed over to a lawyer because he has not paid his account. On these occasions, the order clerk should refer the customer to the credit controller * only the credit controller (not the order clerk) should have the power to remove the "hold" on the debtors account * all "hold" removals should be logged automatically by the computer and the logs subsequently followed up by the financial manager * the system will not allow the order clerk to proceed with the order.
3. Entering and confirming the detail of the order.	3.1 Only once the customer has been validated, can the details of the order be taken. To facilitate the complete and accurate entry of the order, the following programmed (automated) controls should be in place

	* ***screen formatting:*** the screen will be formatted as a sales order * ***minimum entry:*** e.g. entering the inventory item code will bring up the description of the item being ordered and the price. The customer may have the necessary inventory item code on his own system or may have a catalogue (hardcopy or website) which gives the inventory item code, or the order clerk will access the inventory masterfile once the customer has described what he wants to order) * ***mandatory fields:*** e.g. to progress with the order a number must be entered in the ***quantity field***, and a ***customer order reference*** must be entered * alphanumeric check e.g. on the quantity field * limit/reasonableness check e.g. on the quantity field, if applicable * ***screen*** prompts will require the order clerk to confirm details of order and important details such as delivery address and email address with the customer. 3.2 Fields on the "on screen sales order" which cannot be changed by the order clerk, e.g. account number, delivery address, transaction number, are shaded and will not react if clicked on. Mandatory fields have a red star next to the box into which the information must be entered. 3.3 The system will allocate a customer reference number to every sales order which is given to the customer at the time of placing the order. If the customer wishes to follow up on the order or resolve a query, he will quote this number (see Note (a) on the next page).
4. Checking inventory availability	4.1 The order clerk will have read only access to the inventory file. He needs this because he must be able to answer customer queries about availability, alternative products, selling price, etc. The sales order clerk will key in an inventory code or description and the inventory record for the item will appear. (Telesales clerks are not just there to record sales orders. They should have a good knowledge of the company's products and should offer the customer alternatives and try to promote special deals etc). 4.2 If the goods are not available, the order will be placed on a ***back order file*** if the customer agrees (note: the customer may choose to go elsewhere to purchase the goods).

5. Checking creditworthiness (credit approval)	5.1 Once all the details of the order have been entered, the computer will instantly calculate the total value of the sale, add it to the balance on the debtor's (customer's) account, and compare this total to the debtor's credit limit. If the new sale will push the amount owed by the debtor, beyond this credit limit, a screen message will appear alerting the order clerk. The customer will be informed and the sales order can be modified to fall within the credit limit or can be left as it is and placed on a ***pending sales order*** file to await the approval of the credit controller. 5.2 At the same time, the system will check whether the debtor is in breach of his credit terms, i.e. amounts overdue. If so, the sales order will be placed on the ***pending sales order*** file. Note, that an order that exceeds the customer's credit terms or limit, is not automatically rejected. The company wants to make the sale (that is what business is all about) and very often there is a valid reason that the customer has exceeded his credit terms and limit. It does not mean that the customer will not pay. 5.3 If there are no problems with the order, it will be placed on the ***sales order*** file to await the picking process in the warehouse/despatch. 5.4 In some systems, the order clerk may be given authority to override the control which prevents a sales order which pushes the customer past his credit limit, for example, if a R50 000 sales order pushes the customer only R1 000 past his limit, there is little point in upsetting the customer or delaying the sale • if the order clerk has this authority, there will be a programmed control which limits the amount he can override • details of all overrides will be logged. Note (a): In terms of the Consumer Protection Act, once the order has been taken, the company must send a confirmation of the order to the customer which provides details of the order and provides a reference number for the customer to follow up on the order. This can be sent by SMS, email or hardcopy.

Warehouse/despatch	
The picking, packing and despatch of goods are manual procedures. Pickers need a document to indicate which items they must pick.	
Activity/procedure	***Control, comment and explanation***
1. Obtaining the hardcopy picking slip * the warehouse administration clerk will access the sales order file from his terminal in the warehouse. This will reveal a list of sales orders identified by their transaction number. The clerk will "click" on the sales orders he wants to select for picking.	1.1 Access to the sales order file will be restricted • no write access to anyone • no access to pickers • read only access to the warehouse administration clerk • read only access to warehouse supervisory employees • read only access to appropriate management staff e.g. the sales manager. This privilege gives management and supervisory staff the opportunity in a real time system to trace an order from their terminals as it moves through the process. This may be in response to a customer query about an order, or may be to find out if the warehouse personnel are carrying out their duties promptly. 1.2 The sales orders selected, will automatically be transferred from the sales order file, to the picking slip file. In effect the sales order has "become" a picking slip and at the same time, a hard copy picking slip is printed out. 1.3 The sales order will not necessarily be transferred to another file. A common technique is for the system to automatically allocate (attach) a status code to the sales order which indicates that it has been selected for picking and is now at the picking slip stage. Anyone accessing the sales order file will be able to see the status of the original sales order. The code will also prevent the sales order from being selected again for picking.
2. Picking the goods.	2.1 The goods picked are ticked off by the picker against the quantity field on the picking slip, or a number can be entered in a designated field. 2.2 If the quantity of goods required in terms of the picking slip is not available the ***actual*** quantity picked will be entered by the picker on the picking slip against the item. Although a stock availability test was carried out when the order was taken, quantities per the inventory masterfile do not always agree with physical

	inventory. Goods can be lost, stolen or damaged, and errors in the inventory masterfile can occur. 2.3 The picker will sign the picking slip.
3. The goods picked are moved with the picking slip from the warehouse to a transition area.	3.1 A picking control clerk checks the physical goods picked against the picking slip and if there are mistakes (wrong goods picked) or differences between the quantity which has been physically picked, and the quantity on the picking slip, the picking control clerk will go into the warehouse (accompanied by the picker who picked the goods initially) to get the correct goods and confirm that any items short-picked, are actually not available. 3.2 The picking control clerk must sign the picking slip.
4. Correcting and approving the picking slip.	4.1 Access to the picking slip file will be restricted • write access is granted only to the picking control clerk ***and*** • only to the ***quantity*** field • read access is granted to the management and warehouse supervisory staff for purposes explained earlier • read access is granted to the despatch controller • no access to pickers At this point the picking slip on the system will be in agreement with the physical goods picked. 4.2 The picking control clerk will then access the picking slip file and select the transaction number of the picking slip he is dealing with. The screen will come up formatted as a picking slip and the picking control clerk will adjust the quantity field so that the quantity actually picked and the adjusted quantity on the picking slip, agree. 4.3 All quantity adjustments will be logged by the computer.
5. The physical goods are moved to the despatch area. The original picking slip will accompany the goods. It will have been signed by the picker and the picking control clerk and will reflect any quantities short picked.	5.1 Suitable physical protection should be given to goods.

Invoicing	
As discussed in our manual system description, a sales invoice can either be made out and sent with the goods, or it can be made out after the goods have been delivered to the customer. Because controls over accepting and processing orders in an up to date computerised environment are generally very good, there are few problems with delivering the wrong goods or the wrong quantities. This means that businesses can safely invoice the goods before the customer has actually taken delivery. Any delivery problems can be resolved at a later date. In general, the sooner the customer is invoiced, the sooner the business will be paid. In this example, we have assumed that the invoice is made out and sent with the goods. There will usually still be a despatch/delivery note of some kind for the customer to sign, to acknowledge acceptance of the goods, and an additional copy of the invoice will normally be sent to the customer as well (email or hardcopy).	
Activity/procedure	***Control, comment and explanation***
1. Final check of goods before creating the invoice. .	1.1 The despatch controller will access the picking slip file on the system, his access will be read only. 1.2 He will select (click on) the picking slip for the goods he wishes to check, identified by its transaction number or picking slip number • there is no keying in of any information to select the picking slip • the screen will come up formatted as the picking slip. 1.3 The despatch controller will then match the physical goods with the on-screen picking slip and the hard copy picking slip. The goods to be despatched must agree with the on-screen picking slip (as it will be "converted" into the invoice). 1.4 If there are any errors either in the goods picked (wrong goods) or the quantity picked, the despatch controller cannot alter the picking slip or change the goods. The problem must be resolved by the picking control clerk. 1.5 He will also confirm that the picking slip has been signed by the picker and the picking control clerk and then sign it himself. 1.6 The checking of the goods will take place as they are packed for despatch.
2. Creating the invoice	2.1 Once the despatch controller is satisfied that the goods and the on screen picking slip match completely, the despatch controller will select the approve/confirm option and the screen will come up formatted as an invoice. In effect, the picking slip has been converted into an invoice. On selecting the approve/confirm option

	• a hardcopy invoice is printed for inclusion with the goods • a delivery label is printed to be stuck on the box, and the status code on the picking slip on the system will automatically change to indicate that the picking slip has become an invoice (has changed its status) The invoice is transferred from the picking slip file account, and real-time processing takes place on the system, i.e. the debtor's masterfile, sales account and inventory masterfile, are updated simultaneously. 2.2 The approve/confirm option will be restricted to the despatch controller through his user profile. 2.3 The picking control clerk would not be able to approve a picking slip to create an invoice at any stage, e.g. before the despatch controller has carried out his final check. His screen which is linked to his user profile would not reflect an active "approve/confirm" option for him to click on. 2.4 There will be no write access to the file, e.g. nobody, including the despatch controller, will be able to change anything on the invoice.
3. Goods are delivered to the customer. This is a physical procedure and the principles described in the manual system will apply. The most important control is that the customer signs a document to acknowledge receipt of the goods.	3.1 The customer must sign a document (delivery note) to acknowledge that the goods have been received. (Any delivery problems should be noted on the delivery note.) 3.2 This document should be filed in the despatch section in numerical order so that any delivery queries can be followed up.
4. Sales orders on the pending sales order file.	4.1 These sales must be approved or rejected by the credit controller (see section on credit management page 10/35).

Receiving and recording payments from debtors	
In the present business environment, customers (debtors) usually pay by electronic funds transfer from their bank account directly into the bank account of the business to which they owe money. The business receiving the payment in its bank account, now needs to record the receipts as soon as possible so as to maintain its debtors ledger (and cash journal), right up to date. If the company does not keep its debtors ledger right up to date, the debtor's individual accounts will not reflect the correct amount owed and further sales might be lost on the grounds that the debtor has exceeded his credit limits. There are basically two ways in which the company can obtain the details of deposits into its bank account for entry into its accounting records, and both require that the company create a direct link to its bank via the internet. The bank account is accessed every morning and the bank statement downloaded and printed out as hardcopy or downloaded straight into the company's system. If the bank statement is printed out, each deposit will have to be keyed into the system. A daily schedule of receipts will be produced and the detail of each receipt would have to be entered via the keyboard. Even in a highly computerised system, some debtors may still send cheques to the company. In this case, conventional manual receipting controls and depositing would be in place but the entry onto the system would probably be from the downloaded bank statement. This illustration assumes that the bank statement is downloaded directly onto the company's system.	
Activity/procedure	***Control, comment and explanation***
1. Accessing the bank account	1.1 To link the company's system with the bank, the bank will load its software onto a limited number of terminals at the company • one of these terminals will be in the debtors section, usually the terminal of the senior debtors clerk • access to the bank's site will be gained in the normal manner but to access the company's bank account, the senior debtors clerk will need to enter a PIN and password • if this identification and authentication procedure is successful, a menu of the functions available will be displayed, one of which will be "download bank statement" • this function will be linked to the senior debtors clerk's user profile to enable him to initiate the download Note: General access controls will apply, e.g. the terminal should shut down after three unsuccessful attempts to access the company's bank account.
2. Accessing the downloaded bank statement on the system.	2.1 The ability to access (read only) the bank statement file once it has been downloaded, will be restricted to only those who need to work with the bank

	statement, including management and supervisory personnel • the ability to process a receipt should be restricted to the senior debtors clerk.
3. Processing the receipt	3.1 The bank statement should be downloaded each working day so that receipts from debtors (and other items on the bank statement) can be processed promptly to individual debtors so that the debtors ledger is right up to date. 3.2 Debtors should be regularly reminded to • clearly reference their EFT payments when effecting the transfer. This should preferably be a number (not a name) and if possible, the invoice numbers to which the payment refers, should be included. (However, there is only limited space for references on the bank statement) • submit a remittance advice (preferably electronically) to the debtors section. 3.3 When processing the receipts reflected on the bank statement, the senior debtors clerk will work with the references on the bank statement and the remittance advices • there are various ways of processing the receipts, but the invoice number will usually be the "hook". On entering an invoice number, the system will match the invoice number and amount to the file of unpaid invoices and if it finds a match, the debtors account to which the invoice is linked, will come up on the screen • the debtors clerk will select the enter (proceed) option, and the system will update the debtors account in the debtors masterfile and cash book records, as well as the file of unpaid invoices. Note: Potential problems are * the senior debtors clerk cannot identify which invoice is being paid. Without a match to the unpaid invoice file, the system cannot process the receipt * the invoice number matches, but the amount does not, because the debtor has reduced the amount paid by taking an early discount settlement. Again, because there is not a proper match, the system will not process the receipt. 3.4 Any receipt which cannot be matched to an invoice number on the system will be processed to a "receipt suspense file" where it will remain until the problem can be resolved. • removal of the receipt from the receipt suspense file will be restricted to the senior debtors clerk 3.5 Any receipt for which there is a match to an invoice number, but the amount does not match will be written to "a receipt pending file"

	• the credit controller should access this file on a daily basis to determine whether the discount can be approved. The authority to approve will be restricted to the credit controller in the normal manner • if the discount is approved, the receipt will be processed immediately.

Credit management	
Computerisation does not change the objectives of credit management but it can make it far more efficient and effective than in a manual system. The computer is used in a number of ways, e.g. the credit application from the applicant and the follow up of the information can be done online, and the efficiency in the day to day management of debtors can be improved**.** This may involve resolving sales orders and receipt queries on pending files, sending statements by e-mail, identifying slow paying debtors and reconciling accounts. In addition the computer's ability to produce analytical and other reports, e.g. aging schedules, ratios, will be of huge benefit.	
Activity/procedure	***Control, comment and explanation***
1. Granting of credit terms and limits (new customers)	1.1 Regardless of how it is done (online, personal visit), a ***credit application*** must be submitted. The application must contain customer banking details, trade references, financial information • all details should be followed up with bureaux such as, e.g. Transunion or Credit Secure, which will supply an assessment of the applicant's credit rating • online access to a bureaux site will be password protected (supplied on registration with the bureau), and should be known only to the credit controller and his assistant, and must be kept confidential • a credit rating should be obtained directly from the applicant's bank. 1.2 The company should have guidelines for • the credit terms given, e.g. only 30 or 60 days • initial credit limits (to be reviewed after a relationship has been developed with the customer) • handing over a debtor who has not paid, e.g. o amounts owed for over 90 days, handed to a credit agency o large amounts outstanding over 120 days handed over to a lawyer (Note : before handing a debtor to an outside party the credit controller will

	negotiate with the debtor to make payment). 1.3 The final credit terms and limits must be agreed between the credit controller and financial manager in terms of company policy • the terms and limit will be recorded on the credit application form which will be signed by the credit controller and the financial manager.
2. Adding the new customer to the debtors masterfile	2.1 This will be a masterfile amendment and the controls over masterfile amendments described earlier, will apply. The credit application form will be the supporting documentation for the MAF.
3. Approving sales orders on the sales order pending file	3.1 The authority to approve a sales order on the pending sales order file, will be restricted to the credit controller. 3.2 The decision to approve (or not) should only be taken after contacting the client to discuss the matter, reviewing the debtor's payment record, determining whether the non-payment has arisen out of a dispute over a sale and whether there are other pending sales to the debtor. 3.3 The credit controller (and assistants), will have read access to the debtor's account history, e.g. can bring up a list of all previous invoices, payments, current balance, days outstanding, previous payment issues, etc. 3.4 All approvals will be logged and followed up by the financial manager. 3.5 If a pending order is not approved, the customer is notified and the sales order remains on the pending file until the customer can resolve the matter. 3.6 If the sales order is approved, it is transferred to a sales order file for processing in the normal manner. It will no longer appear (or will be suitably status coded) on the pending sales order file to indicate that it has been resolved.
4. Approving discounts (receipts pending file)	4.1 The authority to approve an early settlement discount taken by a debtor should be restricted to the credit controller and should only be given if the discount is in line with the terms and conditions applicable, e.g. • early settlement terms have actually been satisfied • the amount of the discount taken is correct (percentage and calculation) 4.2 All discounts approved should be logged and a report should be generated for review by the financial accountant. Note: If the discount is approved, the system may automatically process a credit note (a report of credit notes generated will be produced).

5. Credit notes and journal adjustments e.g. bad debt write off	5.1 Supporting documentation should be prepared for credit notes and adjusting journal entries and approved by suitably senior personnel. 5.2 All credit notes and journal entries which affect debtors should be approved by the credit controller. 5.3 Access to any credit note or journal entry module should be restricted in the conventional manner, i.e. user profile. 5.4 A weekly report of credit notes passed indicating the reason they were given should be printed out and reviewed by the financial accountant.
6. Debtors statements	6.1 A monthly debtors statement for each debtor should be produced by the debtors department reflecting the state of the debtor's account in the debtors masterfile. Details of all invoices, receipts, credit notes, journal adjustments, should be included as well as a breakdown of the amount owed in days outstanding, e.g. 30 days, 60 days. • debtors statements should be sent or emailed promptly to debtors.
7. Day to day management (reports)	7.1 With modern software a great deal of analysis of information can be carried out on the system and made instantly available to users. The credit management function should make extensive use of these reports, some examples of which are as follows: • new accounts opened • changes to terms and credit limits for individual debtors • debtors exceeding their credit terms and limits • age analyses • debtors payment patterns, etc.

Processing controls

As mentioned in chapter 8, the accuracy, completeness etc, of processing is evidenced by reconciliation of output with input and the detailed checking and review of output by users, on the basis that if input and output can be reconciled and checks and reviews reveal no errors, processing was carried out accurately and completely and only transactions which actually occurred and were authorised, were processed. To make sure it does its job, the computer will perform some internal processing controls on itself, but the user will not even be aware that these are going on. The users within the cycle make use of the logs and reports which are produced relating to their functions, whilst the IT systems personnel make sure that processing aspects of the system are operating properly.

Summary

The description of the system described above, provides an illustration of how the control activities described in chapter 5 (and referred to in ISA 315 (Revised)), can be implemented. It also provides an illustration of how specific automated (programme) controls can be introduced. For example:

Segregation of duties	* Separation of functions, e.g. ordering, warehouse, processing receipts. * Separation of responsibilities within functions, e.g. receiving order, picking, picking control, invoicing.
Isolation of responsibilities	* Isolating responsibilities through granting access privileges, e.g. only credit controller can approve sales orders in the pending sales order file. * Having pickers, and the picking control clerk and despatch controller sign the picking slip.
Approval and authorisation	* A sales order clerk is prevented from proceeding with a sales order unless the customer satisfies the preset credit worthiness requirements. * The financial manager and credit controller approve the credit application.
Custody	* Access to the bank account (custody of the company's money) and the functions which can be performed via the internet, is strictly controlled by user IDs, PINs and passwords. * The information on the debtors masterfile (which is an asset), is also protected by user IDs and passwords to restrict unauthorised amendments.
Access controls	* All users on the system must identify and authenticate themselves by IDs and passwords and what they are authorised to do is reflected in their user profiles.

Comparison and reconciliation	* The system reconciles the allocation of receipts to debtors in the debtors ledger, to the total amount of the deposits into the company's bank account downloaded onto the system. * The system compares current period information about sales and debtors with corresponding prior period information and produces reports.
Performance review	* The realtime processing system allows supervisory and management staff to go into the pending sales order file to see how a sales order is progressing, e.g. to determine whether there is a backlog in picking. * The sales manager accesses the "sales order pending file" to determine whether pending sales orders are being speedily dealt with by the credit controller. * Reports containing information about debtors, e.g. aging, days outstanding, etc, are produced to be compared to performance targets set by the company to measure the performance of credit management.
Control techniques and application controls	* Screen aids and related features • minimum entry : keying in customer's account number brings up all other detail • screen formatting : the picking slip • mandatory fields : customer purchase reference. * Programme checks • validation check on customer number • alphanumeric on quantity field. * Output control • masterfile amendment logs are checked against source documents • access to debtor information on the system is restricted on a "need to know basis".
Logs and reports	* Log of changes made by picking control clerk to picking slips on the system * Daily reports of sales orders received, debtors exceeding credit limits or terms.

This does not cover every control, policy or procedure that could be in place and is not intended to. This knowledge will only be acquired when you go into different companies and work with their systems

9. INTERNAL CONTROL IN A CASH SALES SYSTEM

9.1 Introduction

The making of cash sales presents some unique and difficult risks

* the major risk is loss to the business due to the theft of cash. Cash is easily stolen and to some of those who work with it, the temptation is too great
* this ease of theft can also significantly increase the risk of collusion either with other employees and/or with a customer. For example, in the case of collusion with another employee, a salesman may make a cash sale to a customer, not enter it, and share the proceeds with the security guard whose duty it is to check the goods against a sales docket (in this case there won't be one) before the goods are taken out of the shop. A customer can also easily be drawn into a theft of cash by answering "no" to such questions as "do you want/need a receipt" or answering "yes" to a question such as "do you want to pay cash, because if you do, we don't have to charge VAT." A customer may knowingly or unknowingly answer "yes"!
* the control of cash can be particularly difficult in smaller businesses which don't have the resources to have a strong division of duties or purchase equipment which can assist in preventing some forms of cash theft, e.g. surveillance cameras or sophisticated point-of-sale systems
* in a smaller business, say an owner/managed business, the extent of the desire of the owner/manager to control cash will be a major factor in how well it is controlled. Remember that the owner/manager may be keen to understate his cash sales so as to reduce tax. This attitude also affects the control environment and other employees will soon notice and may even exploit it
* there is also the risk of armed robbery and injury to employees, so cash (at all stages, see 9.2) should be physically safeguarded.

9.2 Stages of a cash sale

For the purposes of describing the controls which should be in place, we will assume that the business has reasonable division of duties and the desire to implement and maintain good control over cash sales. The description will concentrate on ***principles*** as the variations in the nature of businesses which make cash sales are vast, ranging from car washes to food outlets, petrol stations to supermarkets.

A cash sale usually goes through the following stages

* goods or services are requested from an employee of the business, or are selected by the customer to be paid for at an exit point. Typically there is no order document.
* the prices of the goods are rung up on a cash register and a total amount owed is calculated, or a cash sale invoice is created on a computer or manually.
* the customer hands over the cash and is presented with a receipt and change where necessary.
* before leaving the premises, a security guard may check the goods against the receipt/invoice. (This control has practical implications e.g. it is unlikely that groceries are going to be unpacked and checked against the till slip.)
* the cash is kept in the cash till until it is collected for banking.
* the cash is reconciled with a record of sales made, e.g. a till roll and a deposit slip is prepared.
* the cash is banked.
* the cash receipts journal is written up (and subsequently posted to the general ledger).

9.3 Principles of control and examples

* ***physical safeguards*** should be in place to protect cash registers and employees and to prevent theft, e.g.
  - limited exit points and exit points positioned to minimise the risk of a customer leaving without paying as in a supermarket
  - cash not held on an employee's person. Petrol attendants and car wash personnel should take all money to a central secure cash point
  - security guards and camera surveillance
  - signage should encourage customers to request a receipt
* ***an independent record*** of every sale must be kept, e.g.
  - all sales should be "rung up" (entered) on a cash register which retains a total of all ***cash*** sales made. If sales by credit card or cheque are made, it is useful if the record kept by the cash register, records the method of payment for reconciliation purposes

- if a cash sale invoice is printed out on a computer to support a cash sale, a report of daily cash sales should be printed out
- if the system is manual, a cash sale invoice should be written out in an invoice book; one copy given to the customer, one copy retained
- in some businesses a counter of some kind may keep an independent total related to the number of sales which take place, e.g. a car wash bay may keep a running total of cars entering the bay

* ***the independent record should not be alterable***
  - there should be no access to the till roll (or other record) in the cash register in a supermarket, other than to supervisory/management employees
  - handwritten invoices are only protected by the fact that alterations will be visible
  - access to reading, recording and resetting an independent counter (as in a car wash) should be restricted to the manager/owner
* ***the independent record should be sequenced*** so that missing records can be identified, e.g.
  - till rolls or equivalent should be date sequenced (and should identify the cash register they came from)
  - cash sale invoices should be numerically sequenced.
* ***cash should not be allowed to accumulate*** for too long in the cash till (or equivalent), e.g.
  - in a supermarket, cash tills should be emptied regularly during the day and taken to a secure area. This activity may coincide with the changing of the cashier.
  - a car wash manager/owner should ensure that cash is banked every day.
* whenever cash is ***transferred*** from the custody of one person to another, it should be ***counted, reconciled, documented and signed for by both parties*** in a safe location, e.g.
  - when cash is to be removed from a cash register, the till lane will be closed. The cash drawer will be removed by the cashier in the presence of the supervisor and taken by the two of them to a secure back office
  - the two individuals should then count the cash, total the credit card slips and cheques and reconcile them to the independent record which, in this case will be the locked-in till roll (or similar) which will be accessible only to the supervisor. The cash reconciliation would take into account the cash float given to the cashier (and signed for) at the start of the shift
  - the reconciliation should be recorded on a multicopy, pre-printed, sequenced document and should contain information such as date, time, till, cashier name, the actual reconciliation showing any "overs" or "unders", any relevant comments and the signatures of both parties
  - at no stage during the reconciliation exercise, should either of the parties leave the room
  - where there are multiple reconciliations carried out, e.g. lots of tills, the individual reconciliations should be consolidated onto a "daily cash sales" summary
  - the same principles will apply when armed security removes cash for banking
  - in the car wash business, the manager/owner should count the money with the employee responsible for handling the cash, agree the total to the cash sales invoices for the day and the independent counters on the car wash equipment
* ***cash should be banked regularly*** (at least daily) and ***intact*** i.e. cash should not be removed to pay wages or other expenses,
  - a deposit slip should be made out by the supervisor and agreed to the daily cash sale summary (note: cheques will also be banked and must be controlled in the same manner)
  - a second senior staff member should agree the bank deposit slip to the supporting reconciliations and daily summary sheets and sign the documentation
  - the same principles will apply in a smaller business, to the extent possible. A manager/owner is likely to be involved in reconciling and banking of cash
* the cash receipts journal should be written up promptly.
* the financial accountant should regularly inspect the cash receipts journal to confirm that the daily receipts are being banked promptly, and completely, and that the amounts agree with the deposit slips and supporting documentation. The financial accountant will also carefully check the monthly bank reconciliation. All procedures will be acknowledged by signature.

Note 1: Cash registers and point of sales systems have numerous features which assist in the control of cash sales (and other sales). These features relate to some of the principles discussed above, e.g. keeping independent totals, and in addition, will frequently provide reports which can be used for analytical purposes. Reports of cash sales by shift, cashier, salesperson, day of the

week, etc, can be produced. ***Comparison and analysis*** may reveal trends that should be investigated, such as, more frequent discrepancies for a particular cashier, or generally lower sales on the till manned by a particular cashier regardless of which till it is. These modern systems will also produce ***reports of the activities*** which have taken place on the till such as, supervisor overrides, correction of ringing up errors, which can be followed up if they look suspicious, e.g. a supervisor who appears to "override" far more than another supervisor.

Note 2: In some businesses the relationship between cash sales and inventory can provide a good indication of theft of cash. For example, the owner/manager of a fast food outlet may require that, at the end of the business day, cash in the till be reconciled with movement in "food" inventory. If the cash register is able to record separately the different products sold (very common), the number of each product sold can be reconciled with the corresponding inventory on hand. If the outlet started with 500 hamburger patties on hand and ended the day with 100, then the cash register should have recorded the sale of 400 hamburgers. If it only shows 390 sold, 10 hamburger patties are unaccounted for. The cash in the till will agree with what has been rung up, so it suggests that some sales are not being rung up.

In our car wash business, the manager/owner may be able to pick up variances between the month's water and electricity expenses and the number of car washes recorded as sales. More water and electricity used should equal more cars washed. Surprise visits by the manager/owner and cash reconciliations may also reveal irregularities.

These analytical control activities, which are in fact ***performance reviews,*** are not foolproof in themselves, but when combined with further techniques, may become very effective. For example, further analysis may reveal that inventory shortages occur consistently when a particular supervisor is on duty at the fast food outlet.

The point is that where a business has cash sales, a full range of formal controls should be put in place, supported by innovative analysis and follow up.

10. THE ROLE OF THE OTHER COMPONENTS OF INTERNAL CONTROL IN THE REVENUE AND RECEIPTS CYCLE

This chapter has concentrated on the ***information system*** and ***control activities*** components of internal control. However, these components are affected by the other components and a brief mention of the other components is appropriate.

10.1 The control environment.

The tone of the business with regard to control is generally set for the business as a whole by the actions and behaviour of the directors and management and will flow down to the employees in the different cycles which make up the business. Of importance in the debtors section is that senior members such as the sales manager, credit controller and debtors manager, should enforce the controls strictly but fairly and judiciously, especially when a customer is directly involved. For example, a debtor should not simply be handed over for collection to a lawyer without other ways of trying to settle the debt are attempted.

Sales prices should be fair and realistic and the Consumer Protection Act and other relevant legislation should be complied with. The integrity of staff dealing with cash sales and confidential debtor information should be at a high level. Special attention should be paid to controls which address the risk of fraud in the cycle, e.g. invalid credit notes, or debt write offs. In a smaller entity there should be comprehensive owner/management involvement.

10.2 Risk assessment procedures.

Formal risk assessment procedures should address the overall risks faced by the company in the market place, including the promotion of the company's products, methods of selling, sales policies, etc. Less formal risk assessment can be undertaken by the members of the department assessing the risks they face in meeting the function's specific risks as described in the chapter. In smaller entities, it's the owner/manager's informal assessment and response to risks identified in his involvement with the cycle (which is not likely to be particularly strong on formal controls) that will make the difference.

10.3 Monitoring.

Monitoring is about "looking in" on the cycle to determine, over time, whether the internal control system as a whole, is achieving its objective and adequately addressing the risks facing the company. In the context of the revenue and receipts cycle, there are a number of monitoring activities which can take place. Broadly stated, the objectives of the cycle will be to supply customers promptly, with the correct goods at fair prices, to collect amounts owed by debtors according to the terms of the sale and to limit losses from bad debts. These can be monitored by:

* period based comparisons of ratios and statistics such as "debtors days outstanding", bad debt write offs, etc.

* Customer satisfaction can be assessed by customer complaints, the number and reasons for the issue of credit notes, analysis of the buying patterns of major customers, and indirectly by changes in turnover.

NARRATIVE DESCRIPTION OF THE REVENUE AND RECEIPTS CYCLE AT PRORIDE (PTY) LTD

1. INTRODUCTION

The following narrative description is designed to give you an idea of how the revenue and receipts cycle functions in an actual operating company. The name of the company has been changed as have the names of the staff involved. Certain aspects of the company and its systems have been simplified for the purposes of this narrative but in essence, we have described "how it actually happens". Before reading this narrative, we suggest that you read chapter 9 – Computerisation at ProRide (Pty) Ltd.

2. BACKGROUND TO THE COMPANY

The company wholesales bicycles, parts and accessories to the retail trade. Customers include the major chainstores, e.g. Makro, Game, numerous independent bicycle dealers and other general retailers. The company has a turnover of around R140m and about 2 000 debtors. Both foreign and local purchases are made and customers are located mainly in South Africa but sales are also made in other African countries. The company's administrative offices are attached to the warehouse. All goods are received at, or despatched from, the warehouse. The company has a computerised perpetual inventory system with literally many hundreds of inventory items, which are each assigned an inventory item code and a narrative description in the masterfile.

3. OVERALL CONTROL AWARENESS

The company is very "control aware". The tone is set by the senior financial managers who, as you will see later on, monitor all aspects of the business on a continual basis aided by an excellent computerised information system. All the components of internal control (see chapter 5) are present, e.g. there is a strong control environment, sound control activities are implemented and there is ongoing monitoring by senior management. As you read through the narrative you can be satisfied, for example, that the people in the system are competent and trustworthy, there is isolation of responsibility, clear lines of reporting, and all documents used in the cycle are pre-printed, pre-numbered and properly designed.

4. COMPUTERISATION IN THIS CYCLE

This cycle is highly computerised. Sales, debtors and inventory are all run on the IBM AS 400 system, using the JD Edwards software. The company makes daily use of its internet link to its bank to download details of payments made directly into its bank account by debtors so that the debtors ledger can be kept right up to date.

SALES - HOW THE SYSTEM WORKS

It should be noted that great care is taken to ensure that sales orders taken are accurate and complete and that customers are within their credit terms right from the start. This cuts down significantly on problems arising at a later stage. Orders are dealt with promptly; goods will be picked and despatched (usually) within 24 hours. (This is one of the company's performance measures).

1. RECEIVING ORDERS

The company does not make "over the counter" sales. Sales are made to account holders only.

The three order clerks are located in their own office and are equipped with terminals linked to the AS 400, telephones and a direct fax line. They have "read only" access to the inventory masterfile and the debtors masterfile, and for confidentiality purposes not all information on these masterfiles is available to them. All orders are directed to this office.

Orders are received by phone, email, fax and through the post. Orders which are phoned in are not necessarily confirmed by a hardcopy/email order. It should be noted that ProRide (Pty) Ltd's customer base is very varied and ranges from large companies with very formal financial systems, to small general dealers and "bike shops" in small towns and rural areas who have far less formal systems for ordering their goods and paying their accounts.

1.1 Telephone orders

We will assume for the purpose of this illustration that one of the order clerks is Jazelle Roos. When a phone call comes in from a customer, it is directed to the first available order clerk by a phone queuing system.

Validation of the customer

* On receiving the call, Jazelle will greet the caller and enquire as to whether he is an account holder. If so, she will request the customer's account number (or company name) which she will enter onto the system.

* If the number (or name) given by the customer is a match to a debtor on the debtors masterfile, further details pertaining to the customer will appear on the screen and Jazelle will ask the caller to supply (some of) this additional detail to "validate" the customer.

* If the number (or name) given is not a match, no order can be taken.

* If the caller is not an approved customer, the caller will be referred to Judith Oldman, the credit manager.

Debtors with a hold on their account

* When a customer's account details appear, there may be an on-screen message which conveys to Jazelle that the debtor's account is on "hold", meaning that no orders can be taken for that customer.

* The decision to place a hold on a customer's account will have been taken by Judith Oldman (credit manager) and Johan Els (financial manager) and the reason would be that the customer is no longer considered to be creditworthy
  - the hold is effected by the entry of a code into a designated field on the debtor's account in the masterfile (write access to this field is restricted to Judith and Johan and holds are logged for subsequent review by Brandon Nel the financial director)
  - note that this hold has nothing to do with the value of the new order which the customer wants to place, so it is not a matter of a current order pushing the customer past his credit limit. This hold is about identifying a customer with whom the company does not want to trade!
  - if the account comes up with a hold on it, Jazelle Roos will inform the customer and transfer the call to Judith Oldman
  - the hold can only be lifted if Judith Oldman and Johan Els agree, after thorough investigation, that the customer's problems can be resolved. Lifting of this hold is not done until the customer has brought his account into line, and may not even be lifted at this point
  - removal of the hold code is restricted to Judith and Johan, it must be supported by a signed motivation, and is logged for review by Brandon Nel. The intention of this strict set of procedures is to limit losses from bad debts.

Taking an order from a customer

* ProRide (Pty) Ltd does not operate a complete telesales system in that the orders taken over the phone are ***not*** entered directly onto the system. It would probably be more efficient to do so, but the system as it is works well.

* Once Jazelle Roos has "validated" the customer as above, she can take the order details. ***All order details are manually written onto a sequenced, pre-printed internal sales order (ISO).***

* Order clerks are regarded as sales personnel. With many hundreds of different inventory items, customers are frequently not aware of the precise inventory codes and descriptions of what they require despite having access to catalogues, a website, etc. For example, a dealer might wish to order bicycle

spokes; at this point Jazelle Roos will access the inventory masterfile (read access only) and, making use of her "enquiry" privilege, will enter "bicycle spokes". This brings up on screen a list which contains a description of each of the different types of bicycle spoke ProRide (Pty) Ltd carries, the inventory item code, description, number of items in inventory and the selling price. Line items appear as follows:

BS 123	Stainless steel 700c	48	R17.50
BS 149	Galvanised Black 700c	26	R13.20

With this information Jazelle Roos is able to establish exactly what the customer requires, whether it can be supplied (in stock) and the selling price. As each item is agreed, she manually records the item code and quantity on the ISO, and before moving onto the next item, confirms with the customer.

* All order clerks receive ongoing training relating to the products which the company sells. This sound ***personnel practices control*** enables the order clerks to promote sales rather than just take orders. For example, if a customer wants an item but it is "out of stock", Jazelle is competent to offer alternatives. The inventory masterfile also has a field into which additional information can be added (not by Jazelle) to indicate inventory items which may be "on special" at a reduced price. With this information the order clerks can offer these items to the customer.

* Once the order details have been taken, a customer order reference is obtained, and all details of the order are confirmed. The customer is given the ISO number as his reference to the order placed and the telephone conversation is then terminated. Jazelle Roos will then promptly complete the ISO (checking details to the inventory masterfile where necessary) and sign it (isolating her responsibility for taking the order.)

1.2 Backorders

If an item is "out of stock" and a satisfactory alternative cannot be agreed upon, Jazelle Roos will ask the customer whether he wishes his order to be placed on "back order". If so, Jazelle will manually record the details on a back order list. Each week she will access the inventory masterfile to determine whether any inventory items appearing on her backorder list have been received into inventory. Once an inventory item is available she will phone the customer. An ISO is ***not*** automatically compiled. If the customer wishes to place the order the normal procedure is followed.

1.3 Hardcopy orders (fax, post and emails printed out)

All hardcopy orders received through the post are sent by "mail receiving" to the order department. ProRide (Pty) Ltd's customers are provided with the order department's fax number and a dedicated order department email address, and are also requested to mark their hardcopy orders ***confirmation only*** if the order has been placed telephonically. As mentioned earlier, customers do not always confirm telephone orders. All orders which are ***not*** marked confirmation only, are checked against the copies of the ISOs held in the order department to ensure that the order is not duplicated. If there is any doubt, the customer is contacted.

The procedure for hardcopy orders is basically the same as for telephonic orders. An ISO is made out for each order ***after*** the debtor's status and inventory availability checks have been carried out. Thus an order placed by a customer who may have a "hold" on their account will be identified, as will an "out of stock" order. These conditions will be treated in the same manner as a telephonic order.

The result of the procedures in the order department is the production of a source document (ISO) which represents an order from a customer in good standing, accurately compiled and complete with all necessary detail to proceed with filling the order.

2. OPENING OF AN ACCOUNT

As indicated, the company sells only on credit to account holders. Before a business entity is accepted as a customer it must complete a credit application form and submit it to ProRide (Pty) Ltd. (To speed up this process the customer can use the "online" facility available on ProRide(Pty) Ltd's website.)

The credit application form requires the potential customer to provide:

* the business entity's basic details, e.g. name, address, phone numbers, email address, etc
* the business entity's registration number, where applicable, e.g. company or CC registration number
* full details of directors, members (CC) or partners of the business entity
* trade references
* credit terms and limits required.

Judith Oldman (credit manager) then makes use of a credit bureau (which we will call Credit Secure) to investigate the creditworthiness of the potential customer. Credit Secure offers their service "online", and to make use of this facility, ProRide (Pty) Ltd has registered with Credit Secure. On registration ProRide (Pty) Ltd was supplied with a unique password which must be entered once the Credit Secure website has been accessed. The password is only known to Judith and her senior assistant. The website then requires that key details e.g. the company registration number, be entered. This initiates a search of relevant databases and the production of a report by Credit Secure. This report provides ProRide (Pty) Ltd with an assessment of the business entity's creditworthiness as well as a credit rating e.g. A = excellent, E = poor. If Credit Secure has insufficient information about the entity on its databases it will undertake a special investigation if asked to do so.

Once the Credit Secure report is obtained, it is filed with the original application (hardcopy) and discussed by Judith Oldman with the financial manager, Johan Els, at their weekly "debtors" meeting. At this meeting a decision is taken on whether credit should be granted and on what terms. This decision is recorded on a document and signed by both Judith Oldman and Johan Els. The document is used as the authority to add the new customer to the debtors masterfile. Dalene Burger (accounting supervisor) actually enters the new debtor onto the masterfile. All amendments are logged by the computer.

The financial director, Brandon Nel, is supplied with a printout (log) each month of new account holders and he will review the supporting documentation relating to these account holders.

3. THE PRODUCTION OF PICKING SLIPS

3.1 Entering details from the ISO

Once the ISO is complete, it is placed in a secure pigeon hole at the door to the computer department (which is physically separate from the order department). At regular intervals through the day, Rushda Devon, the data clerk, will remove the ISOs from the pigeon hole and capture the details of each ISO to create a "picking slip" (PS). Access to the sales application is restricted. Rushda Devon has her own password and is given read or write privileges to only those modules which she needs to perform her function (least privilege principle). The application is menu driven and Rushda will select the "create picking slip" module. The screen will then come up formatted (laid out) as a "picking slip" and Rushda will enter the information into the appropriate fields. Rushda is required to enter minimal information only, and does not have write access to any fields other than those which she must complete, i.e. she cannot change any standing data e.g. an address. Fields to which she does not have write access are shaded on her screen.

* Entry of the customer's account number brings up the rest of the customer's details
* Entry of the inventory item code brings up the description of the goods ordered
* The quantity ordered must be entered
* The programme automatically provides the document number (sequenced and which cannot be altered) and the date
* The corresponding ISO number must be entered.

3.2 Credit limit check

You will recall that when an order is initially received, any debtor's account which has a "hold" on it is identified, and no sales order will be accepted from that debtor. This is in effect, an initial creditworthiness check and a second credit check takes place when Rushda Devon enters the ISO.

* Once all order details have been entered, the computer instantly calculates the total value of the new order and adds it to the debtor's balance. The new balance is compared on the system to

the debtor's credit limit which is held on the debtors masterfile. (Note that this is only a control procedure, the debtor's account is not updated at this point, nor is a picking slip produced.)

* If the debtor's credit limit will be exceeded if the new order is processed, the picking slip ***cannot*** be printed and the ISO will be written to a sales order ***pending*** file on the system.

* At the same time as the sales order is written to the pending file, a screen message is sent to Judith Oldman (credit manager), alerting her that the sales order is on the pending file
  - as soon as she is able to, Judith Oldman will access the pending file and decide on whether to authorize the sale or not. To be in a position to do so, she carefully considers the payment record of the debtor, the amount by which the limit has been exceeded, and if necessary will phone the debtor to discuss the problem and a possible solution. If she is satisfied in her own mind that the debtor will pay, she will approve the sale. Only Judith Oldman can effect this approval as only a screen linked to her user profile, will reveal the "approve" option
  - on approval, the sales order will be transferred to the picking slip file from where it is treated as a normal approved order. The sales order pending file is updated to reflect that the pending sales order has been approved.

* If on entry of the sales order, the debtor's credit limit check is satisfied (which is normally the case), the sales order is written to the picking slip file. Once Rushda Devon is satisfied with what she has captured, she selects the "print picking slip" option and a picking slip is produced. The printed picking slip contains the following:

  - inventory item code, and description of goods
  - quantity ordered
  - document number and ISO number
  - customer details (including delivery address)
  - an empty block next to the quantity ordered for each item (the actual quantity picked is later entered in this block).

As the picking slips are produced, they are placed in a secure pigeon hole in the picking area. A batch system is not used.

4. PICKING THE GOODS

4.1 Physical picking

* The picking area is located next to the warehouse (see diagram in chapter 12). It is broken down into numerous designated sections where items picked for each order can be placed. It is secure to the extent that only pickers, warehouse management (Reg Gaard, the warehouse manager, and his foreman, Patrick Adams), and senior management are allowed into the area unaccompanied by warehouse management. Patrick Adams closely supervises the team of pickers. Using the picking slip, a picker will take each item from its inventory location (bin, box or shelf) and place it in a designated section in the picking area. Each item which is picked, will be ticked off in the empty block next to the quantity indicated on the picking slip. If the correct quantity cannot be picked the actual quantity picked is entered in the block. The picking slip is signed by the picker and left with the items which have been placed in the designated section of the picking area. Patrick Adams will test check the goods picked against the picking slip on a random basis. (They are checked again at the packing stage).

4.2 Preparing the invoice

* At regular intervals throughout the day, Patrick Adams collects the completed picking slips and delivers them to Dalene Burger (accounting supervisor). She calls up the "prepare invoice" module at her terminal located in the computer department by entering the picking slip number. The "picking slip" appears on the screen and Dalene, with reference to the hard copy picking slip, makes any ***reductions*** to the quantity field that may be necessary. Although an inventory

availability check is done at the order taking stage, situations do arise where the ***theoretical*** "inventory on hand" quantity in the masterfile is greater than the ***actual*** number of items on hand. This could occur where inventory items have been stolen or placed in the wrong inventory location.

* Alterations to other fields on the picking slip cannot be made. For example, additional items cannot be added and any amendment to the quantity field for a quantity which is greater than the quantity field on the picking slip, will be rejected.

* The result of entering the actual quantity of items picked is that the invoice produced agrees exactly with the goods that have been picked for despatch. As you would perhaps expect, details of any quantity reductions entered are automatically written to a report by the computer. The report is used to notify the customer of the problem and for Reg Gaard (warehouse manager) to investigate, before the "stock on hand" field is corrected in the inventory masterfile. Reg Gaard does ***not*** have the necessary access privilege to make the alteration in the inventory masterfile as this would amount to a poor division of duties between custody and record keeping relating to inventory.

* Access to the "prepare invoice" module is restricted to Dalene Burger with Rushda Devon as back up. Once Dalene is satisfied that the "on screen" invoice is in agreement with the hardcopy picking slip, she selects the confirm option. This immediately updates the debtors masterfile and quantity field on the inventory masterfile and the general ledger accounts. The applicable picking slip on the picking slip file is coded to indicate that the goods have been picked and invoiced. She then prints out the invoice in triplicate. The picking slip and invoice have the same document number, but the invoice contains the additional information necessary to record the sale e.g. prices, extentions, value of the sale, VAT, settlement terms, etc.
  - ***Copy 1*** is filed numerically in the debtors section with the picking slip
  - ***Copies 2 and 3*** are sent directly to Reg Gaard (warehouse manager).

* Upon receipt of the two invoices, Reg Gaard and Patrick Adams supervise the packing of the items in each designated section of the picking area, into boxes, checking the goods picked to the invoice. Both copies of the invoice are signed by either Reg or Patrick. One copy of the invoice is placed in the box with the goods, and the second copy is used as a delivery note (see despatch below).

5. DESPATCH

ProRide (Pty) Ltd does not make its own deliveries. The company makes use of a road transport company (Roadline) which delivers country wide on a daily basis. Roadline has a small office staffed by two of their employees situated in ProRide (Pty) Ltd's despatch area (see diagram in chapter 12). The despatch area is physically very secure using conventional methods. The boxes for delivery are moved from the picking area into despatch under the supervision of Reg Gaard or Patrick Adams and one of the Roadline employees. Taking the details off the "delivery note/invoice" the second Roadline employee generates a sticker and waybill (4 copies). Each box is sealed and the sticker, which contains the customer and delivery details (including the number of boxes in the consignment and the relevant invoice number), is stuck onto the box.

The Roadline waybill contains a waybill number, the customer's name and address, the ProRide (Pty) Ltd invoice number and the number of boxes to be delivered to that customer. The 4 copies of the waybill are used as follows:

* ***Copy 1 :*** filed in numerical sequence by Roadline with the ProRide (Pty) Ltd invoice/delivery note
* ***Copy 2 :*** filed in numerical sequence by ProRide (Pty) Ltd. Before the boxes for delivery are finally released to Roadline, Reg Gaard or Patrick Adams checks the details on the waybill to the sticker on the box in the presence of the Roadline employee. Both sign the waybill as evidence of this check.
* ***Copy 3 and 4 :*** go to the customer who signs them to acknowledge receipt of the delivery and returns one to Roadline as proof of delivery.

RECEIPTS – HOW THE SYSTEM WORKS

The vast majority of ProRide (Pty) Ltd's debtors pay by EFT but payments by cheque are still received regularly but not in great numbers. No debtors pay cash directly to ProRide (Pty) Ltd, but a number of the general dealers in rural areas still deposit cash or a cheque directly into the company's bank account.

1. RECORDING AND ENTERING RECEIPTS FROM DEBTORS

1.1 Recording cheques received from debtors through the post

The procedure is as follows :

* Each day's mail is directed to the receptionist, Sharna Pillay.

* At a predetermined time each day, she and one of the purchasing clerks open the post and record details of all cheques received in a remittance register, including date received, name of the business paying the cheque and the amount.

* They sign the register and the purchase clerk takes the cheques and register to Amy Mostert, one of the debtors clerks
  - Amy agrees the cheques to the register and signs the register to acknowledge receipt of the cheques.

* Other post, e.g. orders, correspondence, is placed in secure pigeon holes assigned to various staff members/departments.

* Amy Mostert then completes a preprinted "receipts input sheet" which lists
  - the debtor's name
  - account number and
  - the total amount of the receipt. The total amount is also broken down in terms of the invoices which are being paid. Amy will obtain the detail of which invoices are being paid from the debtors remittance advice or will phone the debtor to find out.

* Before entering the cheque on the "receipts input sheet", Amy will scrutinize the cheque to ensure that it is properly made out and signed to minimize the chances of it being rejected by the bank.

* She will then make out a bank deposit slip for the total amount of cheques to be deposited. She will cross-reference the "receipt input sheet" and the deposit slip and sign the receipts input sheet
  - the cheques and deposit slip are then passed to ProRide (Pty) Ltd's messenger who makes the deposit at the bank
  - the copy of the deposit slip is attached to the "receipts input sheet".

1.2 Recording direct deposits and electronic transfers into the bank account

The same basic procedure is followed for direct deposits and electronic transfers by debtors into ProRide (Pty) Ltd's bank account

* As Amy Mostert does not have any access privileges to the company's banking functions on the internet, Judith Oldman (credit manager) accesses the company's bank account via the internet and downloads a bank statement every morning. (See Chapter 9 for a description of the controls applicable to this procedure).

* The bank statement is passed to Amy Mostert who, assisted by other debtors clerks when necessary, compiles a preprinted "electronic receipts input sheet" in the same manner as for the receipt of cheques
  - all debtors are requested to enter their name and account number as a reference when depositing or transferring money into ProRide (Pty) Ltd's bank account and to

(preferably) email or fax a remittance advice advising exactly which invoices are being paid

- the electronic receipts input sheet is then checked by a second debtors clerk and signed by both debtors clerks.

1.3 Entering the receipts onto the system

The intention is to maintain an up-to-date debtors masterfile. As debtors are debited in "real time" when the invoice is created, it is important that receipts from debtors are also processed as soon as possible. To achieve this, Amy Mostert updates the debtors masterfile on the AS 400 every day.
To do so she

* Accesses the sales application in the normal manner (user ID and password) and selects the "process receipts" module from the menu which appears on the screen which is tailored to her user profile.

* On keying in a debtors account number (taken from the receipt input sheet), the screen will reveal the debtor's account including a list of the unpaid invoice numbers on the account.

* Amy Mostert will select the invoice in respect of which the payment has been received and enter the amount that was paid and is recorded on the electronic receipts input sheet into the designated field.

* If the amount entered does not agree with the amount of the invoice on the system, an on-screen message will appear requesting Amy to confirm the amount. If there are differences between the invoice and the payment received, the detail will be written to a report for subsequent follow up by the debtors clerks. (Note : debtors do not always pay exactly the amount owed; the debtor may make a mistake, or take a discount, etc).

* Once Amy Mostert has entered all the receipts from a specific debtor she will move to the next debtor.

* If there is no invoice listed on the debtor's account in the masterfile against which the receipt can be matched, the receipt is not processed to the debtor's account but is written to a suspense account and subsequently followed up by Amy Mostert.

* When all receipts have been processed, the computer will produce a report showing the total of all amounts entered, broken down into amounts posted to individual debtor's accounts and the suspense account (if any). Amy will agree the total of all amounts entered to the totals on the two receipt input sheets and resolve any discrepancies.

* The system will also produce a listing of all invoices in respect of which the amount received was not correct in terms of the amount reflected on the invoice.

* As each receipt is processed the debtors masterfile and the general ledger accounts are updated.

1.4 Independent reconciliation

* Every Friday afternoon, Johan Els (financial manager) extracts from the system a report of daily receipts processed to the masterfile for the preceding week, and reconciles it to the remittance register, the receipt input sheets, the deposit slips and the bank statement.

* He also extracts a report of all amounts in the suspense account and a report of all invoices in respect of which incorrect amounts were received and which have not been resolved. These reports are discussed with Judith Oldman, the credit manager.

* On the 25th of each month, Amy Mostert produces a Debtors Statement reflecting the state of the customer's account at that date and emails it to the customer (some statements are faxed or posted).

2. CREDIT NOTES AND ADJUSTMENTS TO DEBTOR'S ACCOUNTS

Controls over the passing of credit notes, e.g. for goods returned by a customer, or making adjustments, e.g. writing off a bad debt, are strict

* Every Thursday morning Judith Oldman the credit manager and Johan Els the financial manager will meet to discuss and approve credit notes and other adjustments. A schedule will be prepared based on
  - a list of "customer return notes" (CRNs) prepared by the warehouse department for damaged or incorrect goods returned by the customer. Copies of the CRNs are attached to the list. The sequence of the CRNs is tested following on from the previous week's CRNs and checked for the signature of the warehouse manager (Reg Gaard)
  - the report generated by the computer of invoices for which the correct amount was not paid and the details of the subsequent follow-up thereof. For example, the customer may have taken a discount. If the discount is valid, a credit note will be passed
  - any relevant correspondence from a debtor. For example, a debtor may have been invoiced in error for goods he never received or ordered (seldom happens), or
  - any notification from the company's attorneys that the amount of a long outstanding debt is not recoverable.

* Judith and Johan will prepare the schedule of credit notes and adjustments
  - the schedule will include the debtor's name, account number and the amount of the credit note/adjustment to be passed, and the total of the credits to be passed and the accounts to be debited. The credit notes will also be coded to indicate the reason for passing the credit, e.g.
    Code 1 = incorrect goods supplied
    Code 2 = damaged goods returned
    Code 3 = special discount
  - both Judith and Johan will sign and date the schedule
  - the schedule will be passed to Brandon Nel (financial director) who will scrutinize it carefully, resolve any issues he might have, and sign it to indicate his approval.

* Only Rushda Devon (the data entry clerk) has write access to the "credit note and adjustment module". Access is controlled in the normal manner.

* Once Rushda has accessed the individual debtor's account (by entering the account number), she will enter the details of the credit note/adjustment, working her way through each credit note/adjustment on the schedule
  - normal input controls apply, e.g. minimum entry, validation of debtor's account number, mandatory fields on the credit note code and account to be debited fields. Credit notes entered automatically update the debtors masterfile and general ledger accounts in real time
  - the computer maintains a total of the credits entered which Rushda Devon compares to the total on the schedule once the entering process is complete.

* A copy of the credit note is either emailed to the debtor or printed out and posted or faxed. A copy of each credit note is also printed out to be filed with the schedule and other supporting documentation.

* A day end report which lists all credit notes and adjustments processed and which provides a breakdown of which accounts were debited, is produced. It is reviewed and approved the following morning by Judith Oldman the credit manager.

3. MONITORING

As we mentioned earlier, the control environment in the company is very strong. Over and above the involvement of senior management explained above, the control exercised by Brandon Nel is very significant. He is able to "keep his eye" on the system by making use of up-to-date information which the JD Edwards system can provide. This information is supplied by accessing the system (read access only!) or by the scrutiny of various printouts presented to him, some every day, others every Thursday, and others at month end. The examples given below are not exhaustive but are sufficient to illustrate the point being made.

3.1 Monitoring order picking and invoicing

* Because the above activities are "real time", Brandon Nel is able to access the system at any time during the day and obtain a great deal of information about these functions. For example, he is provided on screen, with the number and rand value of orders entered for the day as well as the gross profit margin on those orders. He can also ascertain at any stage how many of the orders received have been picked and how many have been invoiced. He is also provided with cumulative sales for the day, month-to-date, year-to-date and gross profit for all these cumulative totals, actual and budget. If the process looks to be slow, a phone call or visit to the sales department usually resolves the problem!

* If he wishes, he can call up a list of picking slips that are pending (because the sale pushes the debtor over their credit limit) for discussion with Judith Oldman.

* He can obtain a breakdown of invoiced sales by category, item code, or by debtor, all provided with gross profit margins.

* He also extracts a list of all sales made which produced a gross profit margin of less than 25%. These should only be items which are on "special" or for which there are unique circumstances e.g. bicycles donated as prizes (these are entered as a normal sale with a selling price equal to cost or less).

3.2 Debtors

A great deal of information is instantly available about debtors

* new accounts opened
* debtors who have exceeded their credit limits
* a weekly age analysis
* an analysis of the sales made to the top 200 customers (debtors). Any amount of detail can be extracted, e.g. total value of sales month-to-date, year-to-date and comparisons to the prior year. In addition a breakdown of what items are being purchased by the customer, by description, quantity, value and gross profit margin can be instantly obtained. Brandon Nel uses this to monitor trends. If, for example, sales to a particular debtor are falling, he will attempt to establish why – is the debtor in financial trouble, has he moved his business to another supplier, is he dissatisfied with the treatment he is receiving from ProRide (Pty) Ltd?
* Brandon Nel also receives a weekly report of credit notes which have been entered, broken down into categories (by codes). For example if a large number of "Code 1" credit notes which result from incorrect goods being supplied are having to be passed, an investigation into the picking of goods will result. Similarly, "Code 2" credit notes which result from damaged goods being returned, may indicate a packing or delivery problem or a quality problem.

4. CONCLUSION

It is as a result of these controls that the revenue and receipts cycle at ProRide (Pty) Ltd produces up-to-date, valid, accurate and complete information relating to the totals and balances produced by the cycle i.e. sales, debtors and inventory.

AUDITING THE CYCLE

1. INTRODUCTION

The revenue phase of the cycle is concerned with making sales of the company's products, services or expertise and the receipts phase is concerned with ensuring that the company is paid for supplying the product, service or expertise. Sales can be made in various ways, e.g. for cash, on credit, by instalment and can also be paid for in different ways, e.g. cash, credit card, cheque or electronic transfer. Therefore from an audit perspective, the auditor will need to consider a fair number of aspects relating to the cycle. For example, whether the sale has been appropriately recognized in terms of the relevant accounting statement, whether all cash sales have been recorded and whether the trade receivables balance in the financial statements, is fairly valued.

The audit of this cycle follows the conventional process stipulated in the relevant ISAs. In terms of ISA 315 (Revised), the auditor is required to identify and assess the risk of material misstatement at both financial statement level and at account balance and transaction level. This means in the context of this cycle, that the auditor will need to evaluate whether there is anything in the assessment of risk at financial statement level which may filter down into the audit of the cycle and whether there are any specific risks pertaining to the trade receivables balance in the AFSs or to the recorded sales or receipts (payments) from debtors transactions. For example

* at financial statement level : if there is an incentive for the directors to manipulate the financial statements, one of the ways in which they may do so is by understating or overstating profits by manipulating sales. This can be done in a number of ways, e.g. by creating fictitious sales with related parties, manipulating cut-off at year-end or not recording all cash sales.

* at account balance level : there may be an identified risk that the accounts receivable balance will be overstated because of an inadequate allowance for bad debts.

* at transaction level : risk assessment procedures may have revealed that the controls over cash sales are totally inadequate or that sales invoices are raised before the goods ordered by the customer have even been picked from the warehouse.

Once the cumulative effect of the identified risk has been assessed, the auditor will be in a position to plan "further" audit procedures and "other" audit procedures. Before moving onto the second part of the audit of the cycle, i.e. the response to assessed risk, it is perhaps necessary to remind ourselves of the assertions relating to the transactions in the cycle and the related balance, i.e. trade receivables (which is often referred to as accounts receivable or trade debtors).

2. FINANCIAL STATEMENT ASSERTIONS AND THE REVENUE AND RECEIPTS CYCLE

2.1 Sales

* ***occurrence : recorded*** sales actually ***occurred*** (they are not fictitious) and they pertain to the entity
* ***accuracy :*** sales are recorded at the correct amount
* ***cut-off :*** sales are allocated to the proper accounting period
* ***completeness :*** all sales have been recorded
* ***classification :*** sales are recorded in the proper accounts.

2.2 Receipts

* ***occurrence :*** recorded receipts were actually received for amounts owed to the entity
* ***accuracy :*** the receipts are recorded at the correct amount
* ***cut-off :*** receipts are allocated to the proper accounting period
* ***completeness : all*** receipts have been recorded
* ***classification :*** receipts are recorded in the proper accounts.

2.3 Trade and other receivables

* ***existence :*** trade receivables actually ***existed*** at reporting date
* ***rights :*** the company had the ***rights*** to the trade receivables; i.e. they are not encumbered in any way (if they are, disclosure must be made)

* ***completeness : all*** trade receivables are included
* ***valuation :*** trade receivables have been included in the annual financial statements at an appropriate carrying value (i.e. a suitable allowance has been made for non-recoverable debts).

2.4 Assertions pertaining to presentation and disclosure

In addition to the assertions identified above, the directors are also representing (asserting) that the presentation and disclosure of all matters pertaining to the balances and transactions in this cycle are ***complete*** in terms of the financial reporting standards, have been correctly ***classified*** and ***accurately*** presented and disclosed in an ***understandable*** manner.

3. IMPORTANT ACCOUNTING ASPECTS OF THE REVENUE AND RECEIPTS CYCLE

IAS 18 – Revenue, provides guidance on the recognition of revenue. When auditing a sales transaction, the auditor must confirm that all the following conditions have been met for the sale to have been correctly recognized. These criteria are particularly important where there is an assessed risk that sales may be overstated. If the audit client is simply a wholesaler or retailer, there is not usually much difficulty in determining whether a sale should be recognized but there are some potential complications, e.g. consignment inventory sent to an agent, pre-invoicing, "lay-by" sales and "on approval" sales.

3.1 Sale of goods

A sale should only be recognized if :

* the significant risks and rewards of ownership have been transferred from the seller to the buyer. In a wholesale/retail business, this is usually when the purchaser takes delivery of the goods. Pre-invoicing at year-end to increase sales is not acceptable because it would not satisfy this requirement. Goods given to a customer "on appro" will also not constitute a sale as the customer has the right to return the goods. The risks and rewards of ownership have not been transferred

* the seller does not retain continuing managerial involvement, nor effective control over the goods

* the amount of revenue can be measured reliably. This is usually straightforward as selling prices are calculated and agreed to prior to the sale being made

* costs related to the sale are reliably measurable. Again in a wholesale or retail business, costs are easily measurable as the goods will have been purchased for resale at a specific price

* it is probable that the economic benefits associated with the transactions, will flow to the entity. A company is highly unlikely to sell goods to an entity from which it knows they cannot recover the money. However recording a fictitious sale would contravene this requirement.

3.2 Allowance for doubtful debts

According to IAS 18, when an uncertainty arises about the collectibility of an amount already included in revenue, the uncollectible amount, or an amount for which recovery is no longer probable, should be expensed, rather than an adjustment to revenue being made, i.e. an allowance for bad debts is created rather than reducing the amount of revenue (sales) recorded.

4. FRAUD IN THE CYCLE

4.1 Fraudulent Financial Reporting

There are a number of ways in which management can manipulate account balances and totals in this cycle

* ***creating fictitious sales (occurrence) and the corresponding fictitious debtor (existence)*** – this increases profits and current assets, and improves related ratios

* ***understating sales (completeness) and the corresponding debtor (completeness)*** – the object here may be to reduce taxation or present a less favourable picture of the company so as to reduce the "value" of the company for say, negotiating a management buyout

* ***understating the bad debt allowance (valuation)*** – normally part of a trend of manipulating allowances and provisions to improve profits, assets and related ratios

* ***manipulating the recognition of revenue from sales (occurrence or completeness)*** – rather than create a "fictitious" sale, the company may indulge in activities such as pre-invoicing (raising a sale at year end which is only going to be made or which the company expects will be made in the next financial year, or by recording "lay-by" or "appro sales" as sales). Management may also decide ***not*** to record sales which have actually been made (completeness), depending on their motives.

4.2 Misappropriation of Assets

There are a number of ways in which management or employees can misappropriate assets relating to this cycle

* theft of cash from the cash sales (completeness of sales)

* theft of payments (cash or cheques) received from debtors (existence/valuation of debtors)

* arranging sales to customers at unauthorized reduced prices (accuracy of sales, completeness of debtors/cash) – this is like "virtual theft" from a company and usually occurs when the perpetrator can gain a direct advantage, e.g. he is running his own business "on the side", or the sale is to a friend or family member, or a bribe will be paid over by the person to whom the sale was made

* theft of goods at the picking/despatch stage (existence of inventory) – poor controls over this function may enable warehouse personnel to steal goods by including them in a genuine order, e.g. company A orders 10 items and 15 are picked and despatched. This will normally require collusion with someone "on the outside", such as a friend or relative

* not paying over VAT on all sales (completeness of liabilities) - this amounts to theft from SARS and is not restricted to unrecorded sales (where VAT is very unlikely to be paid), but can occur for recorded sales as well

* making invalid adjustments to debtors accounts (completeness of debtors) – the intention here is to settle a debtor's account without the debtor actually paying, by passing an invalid credit note or writing the debt off as bad when it isn't. This is also normally done where the perpetrator has an interest in the debtor, e.g. a debtor is a friend, family member, or the perpetrator's own business on the side, or where a bribe will change hands

* despatching goods in the normal manner but never raising an invoice. Having the goods despatched in the normal manner, gets the goods (physically) out of the warehouse without suspicion, deliberately not raising the sale makes it theft.

5. FURTHER AUDIT PROCEDURES

5.1 Overall responses to the risk of material misstatement at the financial statement level.

In terms of ISA 330, the auditor must implement overall responses to address risk of material misstatement at the financial statement level. For example

* assigning more experienced staff to the audit, e.g. in response to an assessed risk that management may manipulate the financial statements by the inclusion of fictitious sales with related parties

* emphasizing to the audit team the need to maintain professional scepticism, e.g. to be alert to the risk of unrecorded sales

* providing more supervision

* carrying out procedures in a different manner to prior audits, e.g. carrying out an "early verification" positive debtors circularisation for the current audit when only subsequent receipt testing has been undertaken in the past.

5.2 Tests of control and substantive tests

The auditor's further audit procedures will be a mix of tests of controls and substantive tests. If the auditor intends to rely on the operating effectiveness of controls in determining the nature, timing and extent of substantive tests, he cannot simply assume that the controls have operated effectively, he will need to design and perform tests of controls. If controls prove to have operated effectively, the nature, timing and extent of planned substantive procedures may change, e.g. less testing (smaller samples) may be conducted. The opposite will also apply, that is, less effective controls equals more substantive testing.

5.3 The auditor's toolbox

As we discussed in Chapter 5, in terms of ISA 500, the auditor has the following types or categories of audit procedure available to him

* Inspection
* Observation
* External confirmation
* Recalculation
* Reperformance
* Analytical procedures
* Inquiry

5.4 Significant risks

In terms of ISA 315 (Revised), a significant risk is an identified risk which, in the auditor's judgment, requires special audit consideration. This does not mean that the auditor needs to be familiar with a whole new range of audit procedures (have additional tools in his toolbox), but it does mean that he will look closely at the nature, timing and extent of the further audit procedures which will be conducted, as well as the skills and experience of the audit team.

In the context of this cycle, significant risks may include

* fraudulent financial reporting (understatement or overstatement of sales)
* revenue recognition for complex "sales" transactions such as long-term contracts
* completeness of cash sales in a cash orientated business (supermarket)
* extensive sales to related parties.

6. TESTS OF CONTROLS

6.1 Objective

The auditor tests a control to determine whether the control has been effective in achieving the objective for which it was implemented in the first place. For example, in the context of this cycle, one of the objectives of the controls implemented by the company, will be to ensure that a credit sale is only made to a customer who will pay. To achieve this objective, the controls implemented might include a requirement that a thorough investigation of the customer's creditworthiness be carried out before any sales can be made to the customer. This control will then work in conjunction with other controls which require that all sales orders be approved (signed) by the credit controller before they are executed. In a computerised system, approval of the sales order could be achieved by a combination of programme (automated) controls, e.g.

* a sale cannot be initiated on the system unless the customer is an approved customer on the debtors masterfile (validation/verification check)
* a "hold" (which prevents initiation of the sale) being placed on an approved customer whose account balance is in excess of the customer's credit limit, and
* the "hold" can only be lifted if the credit controller exercises the "approve" option which is granted only to him by his user profile.

Remember that if a sales order cannot be initiated on the system, there will be no picking slip so no despatch, which equals no sale!

The auditor is interested in these controls because if they are effective, the trade receivables balance will contain far fewer debtors who will not pay their accounts, which in turn reduces the risk that trade receivables will be overstated by the inclusion of debtors who are not going to pay (valuation assertion). From an audit perspective, the assessed risk of material misstatement will be reduced which in turn will affect the nature, timing and extent of the auditor's substantive testing. An additional benefit to the auditor is that these controls will also reduce the risk of fictitious sales being made and included in the trade receivables balance. To extend the example, the company may also have a control procedure in place which requires an employee to conduct regular checks that goods which are despatched to a customer, are actually raised as a sale and debited to the customer's account (i.e. despatch notes have resulted in invoices). In a computerised system this may again be achieved on the system, e.g.

* the creation of a despatch note may automatically "trigger" the creation of an invoice
* automatic updating of the debtors ledger.

The auditor is interested in these controls because if they are effective, there is less risk that sales and accounts receivable will be "incomplete". However, as discussed in 5.2, the auditor cannot just assume that these controls (manual or computerised) are effective; he will need to conduct tests of controls to satisfy himself that they are effective.

6.2 Timing

The auditor needs to gain evidence that the controls on which he intends to place reliance were operating effectively throughout the financial year under audit, so tests of controls may be carried out at different stages throughout the year during interim visits to the client. (For some large audit clients such as a bank, testing controls may be an ongoing process.) However, on most audits, to satisfy himself that controls were operating effectively throughout the year, the auditor will rely on the audit trail which is created for the transaction. For example, the auditor could choose a selection of sales transactions from throughout the year and inspect the supporting documentation to see that it consists of an order from an approved customer, a corresponding internal sales order, a despatch note and an invoice, all of which tie up with the description of goods, quantities, dates and document numbers, and which reveal the signatures of employees involved in the process. This of course does not prove that the sale was approved ***before*** it was made or that checking of prices, calculations etc did actually take place, but combined with other evidence the auditor will seek, e.g. whether the debtor paid the amount reflected on the invoice, strong pervasive evidence that the controls were functioning ***at that time*** will have been gathered. If however ***other evidence reveals*** that there are despatch notes for which there is no invoice, or that there are large numbers of credit notes subsequently being issued because incorrect goods are being sent to customers, or incorrect prices are being charged, the auditor gains evidence that the controls (are) were not effective. This is likely to increase the substantive tests which will need to be carried out.

6.3 The nature of tests of controls

As pointed out earlier in the section, the auditor uses an assortment of procedures when conducting tests of controls. Controls in this cycle will vary from company to company and the auditor will need to select a suitable mix of procedures to achieve his overall objective of determining whether the controls implemented were (are) effective. The following procedures are examples of tests of controls which could be carried out :

Inspection

* a sample of recorded sales could be selected and the supporting internal sales order inspected for a valid authorising signature. The inspection of a signed picking slip and despatch note signed by the customer, provides some evidence that the sale did actually occur. The best evidence that the sale occurred would be obtained by inspecting the cash receipts journal/bank statement and customer's remittance advice and matching the recorded sale to the corresponding receipt from the customer. Of course the customer may not have paid in which case the amount should appear in the debtors masterfile
* a sample of credit notes issued to customers could be inspected for an authorising signature and the detail on the supporting documentation, e.g. a customer returns note, could be inspected and matched to the credit note

* the log of masterfile amendments and supporting documentation could be inspected to confirm that appropriate procedures are carried out in respect of evaluating the creditworthiness of new customers before credit is extended, and that the limits and terms granted are approved
* a sample of daily till sales reconciliation schedules (cash reconciled to till rolls) could be inspected and compared to bank deposit slips to determine whether cash sales are banked timeously and in tact.

In a computerised system, the appropriate way of testing programme (automated) controls may be for the firm's computer audit division to conduct system orientated CAATs. For example, the computer auditor may attempt to process an order

* using an invalid customer number
* leaving out a customer order reference number
* inserting an invalid product code
* (or process an order) which will result in the customer's credit limit being exceeded.

Inquiry

* inquire of the despatch clerk as to what happens if goods are transferred from the warehouse to the despatch area for delivery without a picking slip
* inquire of the invoicing clerk as to what procedures he actually follows to ensure that all despatches/deliveries of goods result in invoices being made out
* inquire of the credit manager as to what use he makes of daily reports which are generated on the system of credit notes and other adjustments processed against the debtors masterfile
* inquire of the financial accountant as to whether and how sales to related parties (e.g. companies within the same group) are identified.

Note : questions put to employees should be expressed in a way which requires more than a "yes" or "no" response. In this way the auditor will learn more about the effectiveness of the control and may be provided with information he least expected.

Observation

* observe the despatch clerk counting and checking goods against the picking slip/despatch note before packing items into boxes for delivery
* observe the procedures undertaken at the counter when a cash sale is made, e.g. is the sale rung up
* observe whether gate control personnel actually check goods leaving the premises (being delivered) against the delivery note/invoice.

Note : observation is not a very convincing procedure as the employee is likely to do what he is supposed to do because he knows that the auditor is watching! Observation would always be matched with other procedures, for example in addition to observing the despatch clerk counting and checking, the auditor might inquire of the despatch clerk as to how he resolves a situation where the physical goods for despatch do not agree with the picking slip.

With regard to the testing of controls over the accuracy and completeness of processing and recording of sales transactions and receipts from debtors promptly and in the correct accounts, the auditor takes into consideration that modern software is very fast, efficient and reliable. It is more likely that, instead of reperforming numerous calculations and tracing postings through the system, the auditor will concentrate his tests of controls on the effectiveness of the authorisation/approval of transactions and the effectiveness of controls over reviewing and reconciling the results of processing, e.g. logs, day-end reports, listings etc. This is perfectly acceptable because if the client is using up to date, well supported reputable software, the auditor is most likely to assess the risk of material misstatement arising out of inaccurate or incomplete processing and recording (accuracy and classification, cut-off and completeness) as low.

7. SUBSTANTIVE PROCEDURES

7.1 Nature

In auditing the cycle so far, the auditor will have carried out procedures to

* identify and assess the risk of material misstatement and

* gather audit evidence about the operating effectiveness of the controls (tests of controls).

The auditor is now required to conduct substantive tests which, as we have seen, are designed to detect material misstatement at the assertion level. Substantive tests consist of

* tests of detail of classes of transactions, account balances and disclosures, and
* substantive analytical procedures.

The difference between tests of detail and analytical procedures is that the former consists of auditing the detail of the transactions, account balance or disclosure whilst the latter provide more general or overall evidence. The types of procedure (tests of detail) carried out will still be those listed in point 5.3 with the obvious exception of analytical procedures. For example, in carrying out a test of detail to determine whether transactions in a sample of sales invoices have been allocated to the correct accounting period at the financial year-end (cut-off), the auditor would inspect the description of the goods sold, cross-referencing, ***dates*** and customer signature on the supporting documentation (e.g. internal sales order, picking slip) ***in detail*****,** to confirm that the sale was made prior to year-end. When conducting substantive ***analytical*** procedures, the auditor does not consider the detail but rather the "overall picture". He will compare totals of transactions and balances on accounts period to period, or consider changes in the make up of totals or balances to other periods or industry norms etc, with the intention of identifying any strange or unusual fluctuations. For example, as a "completeness of sales" test, the auditor may compare the total of sales month to month for the current year and to the previous year, and follow up on any strange fluctuations. He may also analyse the accounts receivable balance in terms of the age of debtors (days outstanding) average amount of debt outstanding, and compare the results to the same ratios and breakdowns for the prior year.

In terms of ISA 330, the auditor must design and perform some substantive procedures for each material class of transaction, account balance and disclosure, regardless of the assessed risk of material misstatement. In other words, the auditor cannot decide that there is no need to do any substantive testing because he has assessed the risk of material misstatement for the account heading, class of transactions or disclosures as low, and because his tests of controls provide persuasive evidence that controls had operated effectively for the period under review. The reasons for this are that

* risk assessment is judgmental and the auditor may not have identified all risks, and
* internal control has inherent limitations, including management override, e.g. a member of management may simply override the credit manager and write-off a bad debt which should not actually be written off.

However, the auditor does not necessarily have to carry out both tests of detail and analytical procedures. If assessed risk is judged as low and tests of controls indicate that controls are operating effectively, the auditor may decide that all that is required to reduce audit risk to an acceptable level, is the performance of ***analytical*** procedures. In practice it is more common for the auditor to use a combination of tests of detail and analytical procedures when conducting substantive tests.

7.2 Timing

Most substantive testing takes place at or after year-end. This is logical as these tests are aimed primarily at gathering evidence about the account balances, transaction totals and disclosures in the financial statements. In practice there is often an audit deadline (a date by which the audit must be completed) which forces the auditor to carry out substantive (and other) testing at an interim date, say two months prior to year-end. In the context of this cycle, the auditor may choose to conduct substantive procedures to verify the balance on the trade receivables account at the 10 month period and then "update" this work for the year-end trade receivables account by conducting tests on the remaining two months, during the two months and at year-end. These tests which will be a mix of tests of controls and substantive tests, are termed "roll forward tests". (A reasonably common "early verification procedure" in this cycle is the debtors circularisation).

7.3 Extent of testing

The extent of substantive testing is generally regarded as being a function of (determined by) the assessed risk of material misstatement and the results of tests of controls. In general, the greater the risk of material misstatement and the less effective the controls appear to be, the greater the amount of substantive testing. The extent of testing is usually reflected in the size of samples used for testing.

Overall, the auditor is required to obtain sufficient appropriate evidence to satisfy himself that audit risk has been reduced to an acceptable level.

8. SUBSTANTIVE TESTING OF SALES

The emphasis of substantive testing of sales for the year will often be combined with the substantive testing of the trade receivables balance because they are so closely linked. Of course, if the company makes cash sales, some variations on the procedures conducted will be required. Gathering evidence pertaining to the assertions relating to sales will be achieved by a combination of tests of controls and substantive testing and may be obtained by conducting dual purpose tests.

8.1 Occurrence – recorded transactions have occurred and they pertain to the company

* To obtain evidence that recorded sales actually occurred, the auditor would need to trace a sample of recorded sales transactions back to source and inspect the supporting documentation for the invoice, to confirm
  - that an order was received from an approved customer
  - that a picking slip and despatch note for the goods invoiced, duly signed by the picker and despatcher (and possibly the customer to acknowledge receipt) exist, and that the
  - goods invoiced to the customer were of a type sold by the company.

* The auditor should also trace each sale in the sample through to the cash receipts journal/bank statement and customer remittance advice and by inspection, determine whether a payment of the correct amount for each invoice was received. (If a payment has not been received, the auditor would trace it through to the debtors account in the debtors ledger).

* The results of tests of controls will have a significant effect on the extent of these tests. If for example, tests of controls reveal that the sales initiating and approving controls make it virtually impossible to include a sale that did not actually occur in the accounting records, the auditor's substantive procedures as described above will be reduced.

* In certain instances the auditor may need to give specific consideration to whether the significant risks and rewards of ownership have been transferred from the seller to the buyer at year-end. For example
  - where the goods are supplied to the customer on approval (which means that the customer may return the goods by a specified date if he does not want them.) A sale should not be recognized until the buyer has "approved the goods" or the specified date has been reached
  - where goods have been placed with an agent on consignment, a sale should not be recognized until the agent has sold the goods
  - where a buyer purchases goods but requests that the supplier delays delivery, the sale should not be recognized unless
    - it is probable that the delivery will take place
    - the item "sold" is on hand, identified and ready for delivery to the buyer
    - the buyer has acknowledged the deferred delivery instructions (presumably in writing) and the usual payment terms apply.

* With regard to cash sales, there is usually very little risk that cash sales that have been recorded, have not ***occurred***. There is a far greater risk that cash sales made will not be recorded. This relates to the completeness assertion. However to test occurrence, the auditor may choose to select a small sample of recorded cash sales and trace them to the relevant deposit slip/cash book/bank statement and to the original cash sale invoice/receipt, till roll or daily cash sales spreadsheet.

8.2 Accuracy – the amounts of sales have been recorded appropriately

* As pointed out earlier, the combination of modern accounting software and very reliable hardware, results in transactions which are processed, recorded in and transferred between different accounts, very accurately. The risk that sales are recorded inappropriately will

usually be low. However the computer will process the information it is fed in terms of the "instructions" and controls in the programmes, and despite the low risk relating to the accuracy and classification assertions, the auditor will still need to conduct tests of controls to determine whether the processing of the transactions and the transfer of amounts to the various accounts, is appropriate and executed correctly. To do this the auditor could have a test pack of sales transactions processed through the system. He would then check the results of processing the test pack, against the results which he had pre-determined should have been achieved. An easier way would be for the auditor to select a random sample of invoices and for each invoice

- confirm the mathematical accuracy of the invoice by recalculating all extensions, casts, discounts and VAT calculations
- confirm prices and discounts charged and granted to official price lists or other sources
- confirm that the invoice is a valid tax invoice (e.g. VAT registration number is included)
- agree the quantity and description of the goods invoiced to the quantity and description of the goods on the despatch note.

In effect, these tests will be dual purpose tests in that if the results are as expected, they provide evidence that the controls and procedures are effective and that sales are appropriately recorded.

8.3 Cut-off – the sales transactions have been accounted for in the correct accounting period

The testing of cut-off of sales is designed to establish whether the sales around the year-end were accounted for in the correct period, i.e. sales made after year-end have not been recorded as if they had been made before year-end, or sales which were made before year-end were not recorded until after year-end. The auditor should be aware that management may deliberately manipulate cut-off at year-end to overstate sales or understate sales, depending on their motives. Cut-off can be tested in various ways but will hinge around obtaining evidence about the dates when the risks and rewards of ownership actually transferred. The auditor should

* at year-end obtain the document numbers of the last documents used in the financial year, e.g. sales invoices, despatch notes
* at a later stage he should agree this number to the last entry in the sales journal and sequence test say the last two weeks of invoices before year end, for any missing invoice numbers (these may represent sales which have been made but not entered prior to year-end)
* scrutinize the subsequent month's sales journal for any invoice numbers lower than the cut-off number (none should be found)
* select say the first 20 invoices (or invoices for material amounts) entered in the sales journal for the month after year-end and trace them to the supporting despatch notes/delivery records and by inspecting dates on the documents, confirm that the goods were not actually delivered prior to the year-end
* select say the last 20 despatch notes prior to the year-end cut-off despatch note number and by inspection of the sales journal, confirm that the corresponding sale was raised prior to year-end.

Note :

- if the company receives an order before year-end but only processes (picks and delivers) and records it in the following year, there is no "cut-off" issue
- if the company receives an order before year-end, processes it (picks and delivers it) before year-end but only records it after year-end, there is a "cut-off" issue
- if the company receives an order before year-end, records the sale before year-end but only processes (picks and delivers) it after year-end, there is a "cut-off" issue.

* inspect the cash sales records (e.g. till slips, cash receipts) for say the two or three days either side of the financial year-end and confirm by inspection of the cash sales ledger account and dates on deposit slips, that the sale and the asset were raised in the correct accounting period.

8.4 Classification – all sales have been recorded in the proper accounts

* See comments on "accuracy" above.
* The auditor may also choose to

- test transfers of amounts from the monthly sales journals (both cash and credit sales) to the sales and VAT accounts in the general ledger to confirm that the amounts were posted to the correct account
- inspect the sales account for the inclusion of any amounts which are recorded as revenue, but do not constitute sales, e.g. interest, income, dividend income.

8.5 Completeness – all sales that should have been recorded, have been recorded

The testing for the completeness of sales is difficult because as explained earlier, the auditor is looking for sales which are ***not*** recorded in the accounting records. (The completeness of cash sales can be particularly difficult to audit). When the auditor conducts tests of controls on the sales cycle, he may select a random sample of despatch notes (or even ISOs) and follow them through to confirm that they gave rise to an invoice. This is a completeness test but not one that will help to identify sales that were not even initiated. The substantive procedures which the auditor will conduct for completeness testing will be analytical, e.g.

* analysis of gross profit fluctuations
* comparisons of sales/debtors to prior periods
* analysis of recorded sales by characteristic for comparison to prior periods, e.g. by product, branch, region, month, customer
* comparison of sales ratios to prior periods, e.g. sales commission to sales, cash sales to credit sales.

8.6 Assertions pertaining to disclosure

* Revenue related disclosures are not very onerous but the auditor will still inspect the financial statements to confirm that disclosures are complete, the classification of revenue is correct, the amounts included are accurate and the accounting policies are clearly expressed and understandable.

9. SUBSTANTIVE PROCEDURES FOR THE AUDIT OF TRADE RECEIVABLES (referred to below as debtors)

9.1 Assertion : rights - the company controls or holds the rights to the trade receivable

* By inspection of :
  - prior year workpapers
  - minutes of directors' meetings
  - loan agreements
  - bank confirmations, and

  By enquiry of management :
  determine whether receivables have been factored, ceded or encumbered in any way

9.2 Assertion : existence - trade receivables included in the balance actually exist, they are not fictitious

The two major procedures for existence testing are:

* debtors circularisation by which, with the consent of management, independent confirmation is sought from the debtor

* the matching of amounts owed at year end (receivables) to payments from debtors received after year end. (This is termed subsequent receipt testing). The principle is simple; if a debtor is listed as "in existence" at year-end, and a payment is received after year-end from that debtor, the existence of the debtor at year end is confirmed provided the amount paid subsequent to year-end is in respect of the amount owed at year-end, and not for sales made after year-end.

9.2.1 Debtors circularisation

* the auditor takes control of all debtors statements (at a particular month end) immediately after they have been printed and
  - tests from the statement to the debtors ledger (or debtors schedule/age analysis list) and vice versa, to ensure that a statement has been produced for each debtor and that there is a debtor recorded for each statement
  - selects a sample of statements for circularisation

* two different types of confirmation may be used by the auditor
  - a ***positive*** confirmation requests that the debtor confirms with the auditor whether the balance on the statement ***is correct or not***
  - a ***negative*** confirmation requests that the debtor confirms with the auditor only if the balance on the statement ***is not correct***
* the positive circularisation therefore provides better evidence supporting the ***existence*** assertion e.g. if a negative circularisation letter is not returned it could mean that
  - the debtors balance is correct or
  - that it went to a fictitious debtor or
  - that the debtors balance is incorrect but in favour of the debtor

  The point is that very little evidence is provided by the negative circularisation
* for the sample selected, the auditor encloses in the envelope with the statement
  - a sticker/letter requesting that the debtor confirm the balance directly with the auditor
  - a self-addressed envelope (for positive confirmations only)
* the auditor then supervises the mailing of ***all*** debtors statements and
  - stamps all envelopes to direct "addressee unknown" statements to the auditor's address
  - tests debtors whose addresses are "P.O. Boxes", to confirm that they are not fictitious, e.g. by looking them up in the telephone/business directories and confirming the address with them telephonically
* the auditor thereafter monitors all replies to the circularisation, following up all disagreements and "addressee unknowns" (positive and negative circularisation) and "no replies" (positive circularisation only) so as to collect evidence relating to ***existence*** and to a lesser extent ***valuation***
  - ***disagreements*** should be followed up by reference to relevant source documentation, discussion with credit controller, and if necessary, follow up with the client's attorneys
  - ***"no replies"*** (positive) and ***"addressee unknowns"*** should be followed up by re-circularising the debtors concerned (after correcting the address if necessary), telephone/fax enquiries, and reference to receipts after year-end for evidence of subsequent payment of balances which have not been confirmed.
* errors identified through the circularisation should then be projected over the entire population of debtors to establish the extent of possible misstatement of the overall debtors balance.

9.2.2 Subsequent receipts testing

* a sample of debtors on the year end debtors list is selected
* payments received after year-end from the selected debtors are identified (cash receipts journal)
* these are then traced to debtor's remittance advices to identify which invoices the payment is in respect of
* these invoices and matching delivery notes are then inspected to confirm that
  - they are dated prior to the year-end
  - they were included at year-end in the sales journal and debtors ledger.

9.3 Assertion : valuation and allocation (gross amount) trade receivables are included in the financial statements at appropriate amounts

The valuation assertion for debtors consists of two parts, namely the "gross" amount and the allowance for bad debts.

9.3.1 Gross amount

* the debtors control account in the general ledger should be reviewed for unusual entries e.g. debits arising from journal entries at year-end, and followed up.
* the total on the list of individual debtors should be matched to the debtors control account in the general ledger and the trial balance
  - amounts included on the list of debtors balances should be traced to the individual debtors accounts in the debtors ledger
* if the comparison of the debtors list (per the debtors ledger) to the balance in the debtors control account reveals that there are reconciling items, the following procedures should be carried out on the reconciliation

- casts
- testing of the reconciliation logic
- follow up of reconciling items

* the debtors list should be reviewed for credit balances and these should be followed up and reversed if necessary (material)
* reference should be made to the results of any debtors circularisation and subsequent follow up for evidence of debtor valuation problems, e.g. a debtor claiming that he has been charged twice
* the debtors list and control account should be cast
* for debtors invoiced in a foreign currency
  - obtain the amount of the sale in the foreign currency by reference to the invoice
  - obtain, from a financial institution, the exchange rates at transaction date and at the financial year end date, and multiply the amount by each of the two rates
  - where there is a difference, confirm by inspection of the debtors account, that the balance on the account has been calculated using the financial year end rate (i.e. the currency fluctuation has been accounted for).

9.3.2 Bad debts allowance

* enquiry should be made of the method and procedures adopted by management to estimate the allowance for bad debts
* the authorisation procedure should be established and evaluated, e.g. is it authorised by the credit controller (manager) or the financial director (the more independent of credit control the authorising person is, the better)
* an assessment of whether the basis of calculating the allowance is reasonable and consistent with the prior year, should be made e.g. have circumstances which occurred during the year such as a change in credit policy, been taken into consideration
* all calculations should be reperformed
* the aging of debtors should be reperformed by selecting a small sample of debtors and tracing the amounts owed back to the source documents, e.g. sales invoices and receipts, to determine whether they have been allocated to the correct time period in the age analysis
* all long outstanding debtors and material debtors outside their credit terms, should be identified and discussed with credit management
* the debtors correspondence and legal files should be inspected to identify disputed debtors and debtors who have been handed over
* analytical reviews should be performed
  - comparison of allowance (percentage) to prior year
  - comparison of bad debts written off during the year to prior year
  - comparison of age analysis to prior year, i.e. is debt getting older?
  - calculation of ratios, and investigation of changes year-on-year e.g. days outstanding debtors compared to prior year
* enquiry of management should be made as to any matters which might affect the allowance, e.g. relaxing of the company's credit terms during the year, deterioration in the trading conditions of the business sector of the company's major customers
* the actual bad debt write-offs during the year under audit should be compared to the prior year allowance to obtain an indication of the company's ability to set a reasonable allowance
* all reports given to management (say, on a monthly basis) about debtors should be reviewed e.g. reports on specific debtors who have liquidity problems, lists of debtors written off.

Note (a): Potentially uncollectible debtors should be provided for on a debtor by debtor basis, i.e. an assessment of the recoverability of each debtor should be undertaken. Simply creating an allowance for bad debts by taking a fixed percentage of the gross debtors balance is not acceptable unless there is very strong historical evidence that the percentage chosen is an accurate reflection. Obviously it is only those debtors which display worrying characteristics that need to be considered individually, e.g. long outstanding/disputed debtors.

Note (b): When considering a debtor for recoverability all aspects of the debtor should be considered, e.g. a large chain store may only pay on 90 days, but at the same time the chain store may be a reliable payer.

9.4 Assertion : completeness - all trade receivables which should have been recorded have been recorded

Completeness of debtors is not normally a major concern for the auditor. However, "cut off" testing to confirm that sales, and hence debtors were correctly raised at year end, should be conducted. It is possible that the company delays "invoicing" to the new year to "get off to a good start", particularly if sales targets for the month prior to year end, have been achieved. Analytical procedures conducted on the debtors figures and related accounts also supply evidence of completeness. (See "cut-off" and "completeness" testing dealt with in para 8).

9.5 Assertions relating to presentation and disclosure

* The auditor must inspect the financial statement disclosures and consider whether
  - disclosures are complete in terms of the applicable accounting framework, e.g.
    - the balance is included in current assets (under the heading trade and other receivables)
    - any encumbrances on debtors have been disclosed
  - they are consistent with evidence gathered on the audit
  - amounts, facts, details etc are accurate and agree with the evidence gathered
  - any classification of the information disclosed is appropriate
  - the wording of the disclosures is clear and understandable e.g. the accounting policy and the explanation of any encumbrances.

9.6 Assertions: all, general

An overall analytical review of debtors should be performed e.g.

* comparison of debtors to prior year
* debtors in relation to credit sales compared to prior year
* number and amount of debtors, by division, branch, product.

10. THE USE OF AUDIT SOFTWARE (SUBSTANTIVE PROCEDURES)

If the client's debtors are computerised as they usually are, and suitable audit software is available, the audit of debtors can be significantly enhanced.

10.1 The debtors masterfile can be stratified by rand amount, customer profile etc, and samples selected for circularisation, and/or aging .

10.2 The masterfile can be scanned for "error" conditions:

* duplicated account numbers
* negative balances
* blank fields, e.g. no account number, no name.

10.3 Debtors balances can be independently totalled for comparison with the client's debtors listing total, and totals by monthly break down (aging) can be agreed to the total amount owed.

10.4 Lists of debtors who have a unique characteristic identified on their record can be extracted, e.g. a code may have been added to the debtors masterfile to indicate the debtor has been handed over to the lawyers.

10.5 A comparison of the masterfile at the current year end may be compared to last year's masterfile (if available) to identify :

* new accounts (which could be traced to credit applications to assist in substantiating existence of the debtor)
* major fluctuations in individual account balances
* debtors no longer listed.

10.6 Lists of debtors who have exceeded their credit limits or terms, or a particular threshold can be extracted.

APPENDIX 1

A SCHEDULE OF INDIVIDUAL DEBTORS EXTRACTED FROM THE DEBTORS MASTERFILE OF DO-IT (PTY) LTD AT 30 APRIL 0002

Account number	Account Holder	Address and Contact details	Account balance	Current	30 days	60 Days	60+ Days	Credit Limit	Credit Terms	*Status Code
Ab01	Able CC	4 Pan Rd, Ptown etc	(1 000.00)	2 525.01	(3 625.01)	100.00		5 000	30	2
Am06	Amic (Pty) Ltd	63 Nail Drive, Dbn, etc	6 332.25	3 332.25	800.00	2 200.00		5 000	60	
Bo21	Bow (Pty) Ltd	9 Rep Rd, Dbn. etc	30 046.98			5 870.00	24 176.98	50 000	30	2
Ed07	Edz CC	2 Crox Str, Ptown, etc	78 842.13	47 909.80	15 617.24	12 234.29	3 079.80	75 000	60	
Fi04	Fitt (Pty) Ltd	14 West Street, Westmead, etc	1 097.70	1 097.70					c.o.d.	
Fy01	Fylta CC	221 Box Rd, Dbn, etc	430.94		430.94			500	30	
Ri06	Rite Ltd	12 Wrong Rd, Umbilo, etc	21 090.00	20 040.00	162.01		887.99	20 000	30	3
Ru02	Rubb CC		42 001.50	35 050.00	6 951.50					
Sk13	SK (Pty) Ltd	24 Moon Rd, Chatsworth	93 009.40	49 808.20	43 201.20			100 000	120	
Su06	Sudo Ltd	92 Gate Rd, Hillcrest etc	14 267.00				14 267.00	15 000	30	2
Wi14	Wish CC	41 Golf Rd, Pmb etc	114 298.00	14 100.00		100 198.00		100 000	60	
Ze09	Zed (Pty) Ltd	21 Penn Rd, Bluff etc	3 269.18				3 269.18	4 000	30	1
* Status Code:	1	handed to attorneys								
	2.	current correspondence								
	3.	new account								

APPENDIX 2

PROCEDURES THAT MAY BE CONDUCTED ON THE DEBTORS MASTERFILE OF DO-IT (PTY) LTD USING AUDIT SOFTWARE.

PROCEDURE	ASSERTIONS	EXAMPLE/NOTES
1. Stratify population by amount and express as a percentage of the total population.	-	Amounts : R100 000 and above : between R75 000 and R100 000 etc
2. Scan the entire masterfile and produce reports of "error conditions" 2.1 blank fields (selected fields) 2.2 duplicate account numbers, account holders, address etc 2.3 negative balances 2.4 credit limit field is exceeded by balance field 2.5 debtor has exceeded credit terms 2.6 abnormal credit terms	 existence, valuation existence valuation (gross) valuation (allowance) valuation (allowance) valuation, existence	 Fi04,Ru02 - Ab01 Am06, Ed07, Fi04, Ri06, Ru02, Wi14 Ab01, Bo21, Ed07, Ri06, Su06, Ze09 Sk13, (Fi04)
3. Select samples for 3.1 circularisation (and express as a percentage of total amount receivable) 3.2 account aging	 existence, valuation valuation (allowance)	 samples could be selected from stratification or by debtor characteristic e.g. age, or on a random basis
4. Cast, cross casts	valuation (gross)	Acc balance, age columns
5. Scan the entire masterfile and produce reports of 5.1 code 1 debtors 5.2 code 2 debtors 5.3 code 3 debtors	 valuation (gross and allowance) potentially all assertions existence	 Ze09 Su06, Bo21, Ab01 Ri06
6. Conduct analytical review procedures comparison of current year masterfile with prior year e.g. * age columns as a percentage of total amount receivable * major fluctuations in individual account balances * new accounts	 valuation (allowance) valuation, existence existence	 Is debt is getting older? Auditor must establish reasons Ri06

11. OTHER AUDIT PROCEDURES

11.1 Introduction

In terms of ISA 200, the auditor is required to conduct procedures to comply with all ISAs relevant to the audit, and these procedures are referred to as "other" procedures. An important ISA which the auditor must comply with is ISA 265 which requires that the auditor communicate deficiencies in internal control to those charged with governance. The following paragraphs provide a broad outline of what is required to comply with this statement :

11.2 ISA 265 – Communicating deficiencies in internal control to those charged with governance and management

Objective

* The objective of the auditor is to communicate to those charged with governance and management, deficiencies in internal control which the auditor has identified during the audit and which the auditor believes those charged with governance and management should give some attention to.

Deficiencies

* A deficiency in internal control exists when
  - a control is designed, implemented or operated in such a way that it is unable to prevent, or detect and correct misstatements in the financial statements on a timely basis, or
  - a control necessary to prevent, or detect and correct, misstatements in financial statements on a timely basis, is missing.

Significant deficiencies

* ISA 265 draws a distinction between deficiencies and ***significant*** deficiencies and the reason is that the parties to whom they are reported will differ
  - the general rule is that all ***significant deficiencies*** will be communicated to those charged with governance and to management
  - however, if it is not appropriate to communicate directly with management, the auditor should not do so. This situation will arise where the significant deficiency may "call into question" the competence or integrity of management
  - deficiencies which are not significant, will be reported to management if, in the auditor's opinion, the deficiency is of sufficient importance to merit management's attention (but not so important that those charged with governance need to be communicated with).

Determining significance

* For a deficiency to be significant does not require that a misstatement must have already occurred. Although a misstatement may have occurred, the auditor is also concerned about the ***potential*** for misstatement to occur, and alerting those charged with governance so that the deficiency can be responded to and potential misstatement prevented.

* A number of deficiencies which individually would not be significant may be significant when considered collectively.

* The following matters, inter alia, will be considered by the auditor in determining whether a deficiency is significant
  - the likelihood of the deficiency leading to material misstatement
  - the susceptibility to loss or fraud to which the deficiency gives rise
  - the volume of activity associated with the account balance or class of transaction which is affected by the deficiency
  - the importance of the "deficient" control in relation to the financial reporting process, e.g. deficiencies in controls over the prevention of detection and fraud, or the identification of related party transactions, or year-end journal entry approval may tend towards being significant.

* Indicators of significant deficiencies in internal control include
  - the suspected presence of management fraud

- lack of action or concern by management in responding to deficiencies communicated
- inadequate company risk assessment processes or a failure to respond to risks timeously or at all
- detection of misstatements by the auditor – proof that the system is not "working".

Content and form of the communication

* Significant deficiencies should be communicated in writing (not orally)

* Communication with management of non-significant deficiencies may be oral (less formal). For example, they could be communicated in a meeting with management and should be recorded in the minutes of the meeting

* The communication should contain
  - a description of the deficiencies and an explanation of their potential effects
  - an explanation that the purpose of the audit was to express an opinion on the financial statements, and ***not*** for the purpose of expressing an opinion on the effectiveness of internal control, and
  - that the deficiencies being reported are limited to those identified during the audit that the auditor has concluded, are of sufficient importance to merit being reported to those charged with governance.

12. SUBSTANTIVE PROCEDURES FOR THE AUDIT OF BANK AND CASH

12.1 Introduction

* Some companies may have numerous bank accounts. For example, a company may have :
  - a number of branches around the country each of which has its own bank account. All the company's bank accounts could be with the same bank (e.g. Absa), or different banks (e.g. Absa and Nedbank)
  - a main bank account and a number of "clearing" accounts such as a salaries account
  - a number of different types of bank account, e.g. a current account, call accounts, a deposit account.

12.2 Cheques and EFTs

* The huge increase in the use of EFTs has resulted in a very significant decline in the number of cheques which are passed between businesses. This combined with the fact that EFTs are reflected almost instantaneously in the company's bank account, has resulted in the company's "cash book" balance and the balance "per the bank statement" being closely aligned particularly where the company downloads bank statements frequently to update its cash book for EFTs into its bank account.
  - For example, if a company pays its creditors by cheque say, two days before year-end, sends the cheque to the creditor who then banks the cheque, there will be a relatively long delay before the cheque is cleared through the bank. For the period that the cheque remains uncleared, the company's cash book and the corresponding account at the bank will not agree. If the company pays its creditors by EFT even on the last day of the financial year, the company's account at the bank will reflect the payments and the cash book and bank account balance will agree.
  - A similar situation will apply to cheques received directly from debtors; the company may enter the receipts in the cash book but only make the deposit into the bank account a few days later. For the period that the cheques remain un-deposited, the cash book and the bank account will not agree. If the debtor pays directly into the company's bank account by EFT and the company records the receipt promptly in the cash book (which it should), the cash book and the bank account balances will agree.

* However, some companies do still pay creditors etc by cheque and still receive cheques from debtors, so outstanding cheques and deposits do still appear on year-end bank reconciliations. It is also possible that a year-end bank reconciliation could include a number of EFTs as reconciling items. This will happen where the company prepares the EFTs, enters them in the

cash book, but does not "release" the payments until after the year-end. As the EFT has not been processed by the bank at year-end, the cash book and bank account balances will not agree.

12.3 Window dressing

Window dressing is the intentional manipulation of the relationship between balances in the current assets and current liabilities section of the statement of financial position. If done intentionally, the example of preparing and entering EFT payments but not releasing them for payment would be window dressing. Consider the following example :

	Cash book	***Creditors***	***Ratio***
Balance without window dressing	100 000	50 000	2:1
Prepare EFTs but do not release	25 000	25 000	
Balance with window dressing	75 000	25 000	3:1

If a company pays its creditors by cheque exactly the same principle applies, the cheques would not be sent to creditors until after year-end.

12.4 Procedures (bank accounts)

Assertion : rights, existence and completeness

* Obtain a schedule of all bank accounts held by the company at year-end
  - compare the accounts listed on the schedule to the prior year schedule and note any changes.

* Obtain a bank confirmation from the bank. Refer to Chapter 17 – External confirmations from financial institutions – SAAPS 6

Assertion : valuation

* Agree the balances for each bank account on the schedule to the balances in the general ledger and cash book(s).

* Agree the balances on the reconciliation to the cash book, bank statement and bank confirmation balances respectively.

* Reperform the casts on the reconciliation and at the same time, test the logic of the reconciliation.

* Trace reconciling items through to the cash book prior to year-end, and agree the amounts and dates.

* Trace reconciling items through to the post year-end bank statement to confirm that they went through the bank and were not cancelled.

* Where reconciling items are anything other than immaterial, request the client to reverse the items, particularly if there is any suggestion of window dressing, e.g. EFT payments recorded in the cash book but not actually paid until after year-end.

Note (a) : Where the company makes material transfers close to the year-end, between its own bank accounts held at different banks and between its own bank account and other related party bank accounts, e.g. a subsidiary's bank account, the auditor should

* compile a schedule of all movements between the various accounts
* confirm by reference to source documentation and enquiry, that the transfers are in respect of valid arms-length transactions and
* that the transactions are properly accounted for in the correct period, i.e. the payments and receipts from and into the respective bank accounts are accounted for in the same accounting period.

Note (b) : Because the risks associated with EFT payments can be so high, the auditor may at this stage, decide to select a random sample of EFT payments from the bank statements to confirm the validity of the

bank account details to which the payment was made. Audit work will have already been done on this when substantive tests on payments were conducted, but the auditor might wish to supplement his "cash at bank" testing. For this specific test it is not sufficient to refer solely to payee documentation, e.g. an invoice. With current accounting packages, it is very easy to duplicate the standard invoice produced by these packages, but to change the banking details on the invoice. The procedure would be to confirm the banking details ***directly*** with the payee.

12.5 Procedures (cash on hand)

The majority of companies do not have large amounts of cash on hand at year-end, but some companies do, e.g. a supermarket or hardware store which does a lot of cash trading with the public. At year-end there may be a fair amount of cash on hand which has not yet been banked and which the auditor might decide to count. In these types of business, the company will count cash in the tills at the end of the day and agree the takings to the total kept by the cash register. The takings from each till (adjusted for any floats) will be entered on a till count reconciliation and subsequently onto a daily spreadsheet of takings. The spreadsheet will be cast and cross-cast and a deposit slip will be made out. A security company will usually collect the takings for banking. If the auditor decides that the cash on hand should be verified, he should

* be present at the time(s) the cash in the tills is counted
  - he should make sure that at no time is he left on his own with an open till (could be accused of theft if there is a shortfall)

* observe the counting of cash closely, ensuring that cash, credit card slips and cheques are separately identified

* confirm that the totals of the different types of sales (cash, cheque, credit card) counted, agree with the totals recorded on the (independent) till roll total and that any differences are recorded on the till reconciliation document and that the cashier and the controller (person doing the counting) sign the till roll and the reconciliation

* ensure by observation that the cash from the first and subsequent tills counted is kept separate and secure and cannot be included in the cash counted for other tills, and that the tills which have been counted, are closed/deactivated

* confirm by inspection, that the takings for each till (per the reconciliation) were entered accurately on the daily spreadsheet and reperform the casts and extensions

* obtain the spreadsheet for the two trading days prior to the current trading day and confirm that takings for these days were banked prior to the year-end

* inspect the bank deposit slip for the current day's takings (cash and cheques) and agree the totals for cash and cheques to the daily spreadsheet

* inspect the bank statement subsequent to the year-end and confirm that the deposit went through the bank

* a workpaper should be created which records the balances and other details

* confirm by inspection of the respective ledger accounts, that these cash sales/VAT were included at the year-end.

12.6 Disclosure

The disclosure of bank balances and cash on hand is relatively straight forward

* the total will be shown on the face of the statement of financial position under current assets (other than bank overdrafts) under the heading "cash and cash equivalents"
* this will be supported by a note which will distinguish between the different categories, e.g. cash on hand, current account balances and call account balances
* the details of any security, pledge, etc offered, attached to a bank overdraft will also be disclosed.

CHAPTER 11

ACQUISITIONS AND PAYMENTS CYCLE

CONTENTS

		Page
THE ACCOUNTING SYSTEM AND CONTROL ACTIVITIES		
1.	Introduction	11/2
2.	Characteristics of the cycle	11/2
3.	Objective of this section of the chapter	11/2
4.	Basic functions for any acquisitions and payments cycle	11/2
5.	A narrative description of a manual acquisitions and payments cycle by function	11/3
6.	Documents used in the cycle	11/5
7.	Flowcharts for a manual acquisitions and payments cycle	11/6
8.	Computerisation of the acquisitions and payments cycle	11/14
9.	The role of the other components of internal control in the acquisitions and payments cycle	11/31
THE ACQUISITIONS AND PAYMENTS CYCLE AT PRORIDE (PTY) LTD		11/32
AUDITING THE CYCLE		11/41
1.	Introduction	11/41
2.	Assertions and the acquisition and payments cycle	11/42
3.	Fraud in the cycle	11/42
4.	Further audit procedures	11/43
5.	Tests of controls	11/44
6.	Substantive procedures	11/46
7.	Substantive testing of transactions in this cycle	11/47
8.	Substantive procedures on the trade and other payables balance	11/49
9.	Other audit procedures	11/52
10.	The use of audit software (substantive procedures)	11/52

THE ACCOUNTING SYSTEM AND CONTROL ACTIVITIES

1. INTRODUCTION

The acquisitions and payment cycle deals with two major activities which are linked but which are also quite distinct, i.e.

* the ordering and receiving of goods (or services) from suppliers, and
* the payment of amounts due for the goods ordered and received

The acquisition phase of the cycle attempts to ensure that the company orders and receives only those goods which it requires and that the goods are of a suitable quality and price. The second phase of the cycle attempts to ensure that ***only*** goods that have been validly ordered and received, are paid for and that payment is authorised, accurate and timeous. The cycle is also referred to as the purchases and payments cycle.

This chapter deals initially with the accounting system (which is part of the information system) and the control activities which are put in place to achieve the above objectives.

The latter part of the chapter deals with the audit of the cycle.

2. CHARACTERISTICS OF THE CYCLE

2.1 Importance of the cycle.

Goods and services are acquired by a business for resale or for manufacture of a product, so the consequences of a poor acquisitions cycle will have a very negative effect on the business. If the correct products are not available, sales will be lost and production may be halted. It will not be long before the company gets a reputation for being unreliable and customers will go elsewhere. Purchasing goods that do not sell or which cannot be used because of demand or quality issues will also result in losses. It is important therefore, that the correct goods of the required quality and price are acquired and that they are received timeously.

2.2 Susceptibility to fraud.

* The cycle includes procedures which facilitate the payment of creditors which means that there will be the necessary mechanisms to facilitate an ***outflow*** of funds from the business. Stealing from the company through the official payment system may be considerably easier than say, stealing inventory or creating fictitious workers to steal wages. For example, if creditors are paid by electronic funds transfer and controls are not extremely tight, theft from the company's bank account in the form of a payment to a fictitious creditor can be effected very quickly and efficiently.
* The cycle is also fertile ground for corruption. Suppliers may offer the company's directors or buying department employees, bribes or other illegal inducements to purchase their products. Senior personnel may engage in tender fraud, e.g. awarding tenders which are significantly inflated to suppliers, and sharing the "extra" profits made by the supplier in their personal capacities.

3. OBJECTIVE OF THIS SECTION OF THE CHAPTER

Our objective in this section of the chapter is to provide you with the necessary information on how an acquisitions and payments cycle might work. In practice, acquisitions and payment systems will vary considerably depending on the products the company sells or manufactures, its size, whether or not it imports goods, the software used by the company, and a number of other factors, but all systems must adhere to the basic principles. Our approach is to get these basic principles across to you by dealing with an easily understandable manual system, and then describing how computerization can be introduced into the system. Computerisation does not change what is required of the system but it does change how it is achieved.

4. BASIC FUNCTIONS FOR ANY ACQUISITIONS AND PAYMENTS CYCLE

4.1 Ordering of goods

* There must be a section or department which initiates the placing of orders for goods or services with suppliers. Requests for orders to be placed will come from other departments, e.g. the warehouse (stores) department, the accounting department (stationery, etc).

4.2 Receiving of goods

* This function will be responsible for receiving goods ordered from suppliers and acknowledging the company's acceptance of the goods.

4.3 Recording of purchases (acquisitions)

* The purpose of this function is to raise the purchase and the corresponding liability (creditor) in the accounting records.

4.4 Payment preparation

* This function will be responsible for determining the amount to be paid to the creditor, confirming that the payment is valid and preparing any documentation required for the payment to be authorized and initiated.

4.5 Actual payment and recording of the payment

* This function will be responsible for preparing the means of payment, e.g. cheque or electronic funds transfer, authorizing it and carrying out the payment timeously.
* The function will also be responsible for recording the payment in the accounting records.

5. A NARRATIVE DESCRIPTION OF A MANUAL ACQUISITIONS AND PAYMENTS CYCLE BY FUNCTION

5.1 Ordering

The purpose of this function is to place ***approved*** orders with suppliers to obtain goods (and services) which the company requires. The majority of goods ordered will be either inventory for resale or raw materials for manufacture. However, other departments such as maintenance, accounting, sales and security, also require items on a regular basis and these should also be ordered through the company's purchasing system. The ordering function is essentially responsible for obtaining the correct ***type*** and ***quantity*** of goods at the best ***price*** and desired ***quality***. Many companies have what are termed "approved suppliers" from whom goods are purchased. Before being placed on the approved supplier list, the supplier will be thoroughly investigated for reliability of delivery, quality and price. Company buyers also build up relationships with particular suppliers over time who become "informally" approved suppliers.

Besides the obvious problems which arise out of inaccurate or late ordering, management needs to be aware of the risk of buyers deliberately placing orders which are not at the best price and quality from the company's perspective, so as to earn "kickbacks" or "commissions" for themselves, at the expense of the company. Buyers may also place orders at inflated prices with their own businesses, or those of a family member or friend, again at the expense of their employer.

* in a manual system, hardcopy requisitions from departments requiring goods of some kind will be delivered to the buying department
* the buying clerk will manually complete a multicopy pre-printed, sequenced purchase order after checking with the supplier as to availability and price of the goods to be purchased, and referring to supplier catalogues for descriptions and codes
* the buying clerk may refer to a hardcopy list of approved suppliers or may choose a supplier himself
* a chief buyer may scrutinize all purchase orders and approve them by signing the document
* the order will often be placed by phone, and a hardcopy sent as confirmation by fax or post.

5.2 Receiving

* the role of the receiving function is to accept goods from suppliers and acknowledge receipt thereof. Only goods for which valid purchase orders have been placed, should be accepted. In the real world, the receiving function often proves to be the weakest link. The usual way of perpetrating fraud in this area is for the supplier's delivery personnel to deliver only say, half of the truckload, but for the receiving clerk to sign for a full truckload. The goods which remain on the truck, are then driven off the premises and sold cheaply for cash, before the supplier's driver returns to the supplier's depot. The receiving clerk and supplier's driver share the proceeds from the sale of the stolen goods. Obviously this requires collusion between the supplier's delivery personnel and the company's receiving and warehouse personnel, and perhaps highlights collusion as the major limitation of internal control.

* a copy of all purchase orders will be sent to the receiving bay and filed in numerical sequence
* on arrival of the goods from the supplier, the receiving clerk will match the purchase order reference on the suppliers delivery note to the purchase order to determine the goods to be received
* the receiving clerk should count the goods received against the delivery note and purchase order and should perform at least a superficial check of the quality of the goods. It is usually not practical to quality check the contents of boxes, but obviously damaged or wet boxes should be rejected. Any deliveries which are incorrect or rejected will be clearly marked on both copies of the suppliers delivery note and the amendment signed by the supplier's employee and the receiving clerk
* the receiving clerk will make out a sequenced goods received note for the goods actually received, cross referencing it to the purchase order and delivery note
* the goods will then be transferred from the receiving bay, which should be a physically separate section of the warehouse, to the inventory department who are responsible for the custody of the inventory.

5.3 Recording of purchases and creditors

* the purpose of this function is to record the purchases made and the corresponding creditor for all purchases, accurately and timeously.
* the purchases will be entered in the purchase journal and allocated to the correct account to be posted to the general ledger and creditors ledger
* before being entered, the invoice sent by the supplier should be:
  - matched to the purchase order, supplier delivery note and goods received note, and inspected for signatures of employees who perform a control procedure, e.g. the chief buyer
  - checked against supplier price lists or prices quoted on the purchase order
  - checked for accuracy of casts, extensions, discounts and VAT
* all of the above will be performed manually on hard copy documentation. A copy of each of the documents used, e.g. customer order, will have been sent from the originating function/section and filed in a temporary file awaiting the arrival of the invoice from the supplier.

5.4 Payment preparation

This is an extremely important function because if it is not controlled properly, invalid payments can be made. All supporting documentation, i.e. order, delivery note, goods received note and invoice, should have been matched as above and will now be reconciled to the creditors statement and the creditors account in the company's creditors ledger by employees in the creditor's section. Creditors are normally paid once a month and not as individual invoices arrive (although payments may be made on the strength of valid invoices before any reconciliation to the creditor's statement is carried out).

* normally a creditor's statement will be sent by the supplier towards the end of the month. The statement will reflect the balance owed to the supplier at the start of the month, all invoices issued and all payments received as well as any adjusting entries, e.g. credit notes passed by the supplier for goods returned, and the balance owing at the end of the month. This balance owing will be broken down into the periods for which it has been outstanding, e.g. current, 30 days, 60 days
* the creditors statement will be reconciled with the supporting documentation and the creditors account in the company's creditors ledger
* a schedule of "payments to creditors" will be prepared and cheque requisitions and remittance advices made out.

Note: It is, of course, possible that payments could actually be made by electronic funds transfer in an otherwise manual system.

5.5 Actual payment and recording of payment

* this function which should be solely responsible for actually making the payments to creditors, whether it be by cheque or EFT. The function will also be responsible for recording the payment. Note, that cheque signatories and those responsible for approving and releasing electronic payments will be independent of the payment preparation procedures, e.g. the same individual should not prepare and sign the cheque, there should be as split between preparation and approval.

* an employee in this function will write out a cheque for each creditor and present the cheques to the signatories with the supporting documentation for approval (signature)
* the cheque and remittance advice will then be sent to the creditor
* the cash payments journal is written up and the payments subsequently entered in the creditor's ledger and general ledger

6. DOCUMENTS USED IN THE CYCLE

6.1 Requisition.

This document is used to convey to the buying department, that goods are required. The requisition can be initiated in any department but will mainly come from the warehouse department. How the warehouse department determines when goods are required varies, but the most common ways are :

* the use of re-order levels and re-order quantities. Each inventory item is assigned a re-order level and a re-order quantity and as soon as the re-order level is reached, a requisition for the re-order quantity is prepared by the warehouse department. This presupposes that some kind of perpetual inventory recording system is maintained. Alternatively warehouse personnel could perform regular counts of physical inventory and compare quantities on hand to re-order levels. Not very efficient! Using re-order levels and quantities will be far easier in computerised perpetual inventory systems where the computer can be programmed to print a daily report of inventory items which have reached their re-order level
* the use of production schedules which indicate when particular inventory items are required
* by particular request (preferably written), from a manufacturing or other department.

6.2 Purchase order forms.

Purchase order forms which are completed by the buying department, record the detail and price of the goods to be purchased and are addressed to the supplier. They should be signed by the chief buyer.

6.3 Suppliers delivery note.

This document is made out by the supplier and details the goods which are being supplied. It will be cross-referenced to the purchasing company's order form and on delivery of the goods, will be signed by the purchasing company to acknowledge the receipt of the goods.

6.4 Goods received note.

This document is completed by the purchasing company when the goods are delivered by the supplier. It records the actual goods received and will be cross-referenced to the suppliers delivery note.

6.5 Purchase invoice.

This document is sent by the supplier to the purchasing company to inform them of the goods for which it is being charged, the price, any discounts and VAT.

6.6 Credit note.

This is a supplier document which records any credits to the purchasing company's account other than a payment, i.e. when incorrect, damaged or unwanted goods are returned by the purchasing company. Returned goods should be accompanied by a ***returned goods voucher.***

6.7 Creditors statements.

Produced by the supplier on a monthly basis; this document summarizes the transactions between the supplier and purchasing company for the month, in terms of the supplier's records.

6.8 Cheque requisitions.

A form completed by the creditors section of the purchasing company requesting that a cheque be made out for a particular creditor. Details of the creditor and amount to be paid will be shown on the requisition.

6.9 Remittance advice.

A document sent by the purchasing company to the supplier which contains a breakdown of the invoices which are being paid by the accompanying cheque (or bank transfer).

6.10 Receipt.

A document provided by the supplier to acknowledge that a payment of Rx has been received.

6.11 Logs, variance reports, etc.

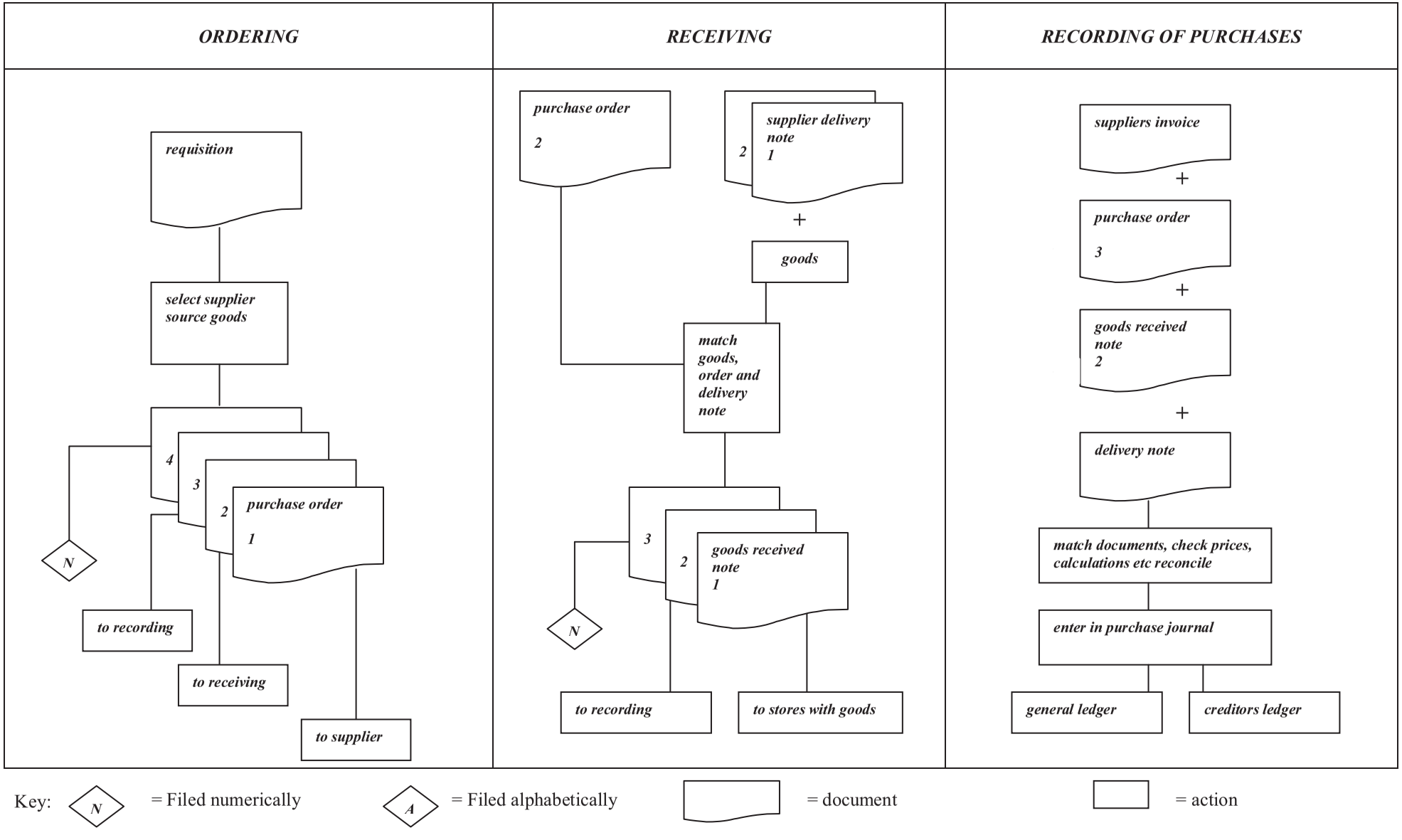
In a computerised system, the computer can be programmed to compile logs, variance reports, lists, etc. A log is simply a record of an activity that has taken place on the computer, e.g. if a masterfile amendment is made, the computer will automatically "store" the activity, who did it, when and where it was done and the nature of the amendment.

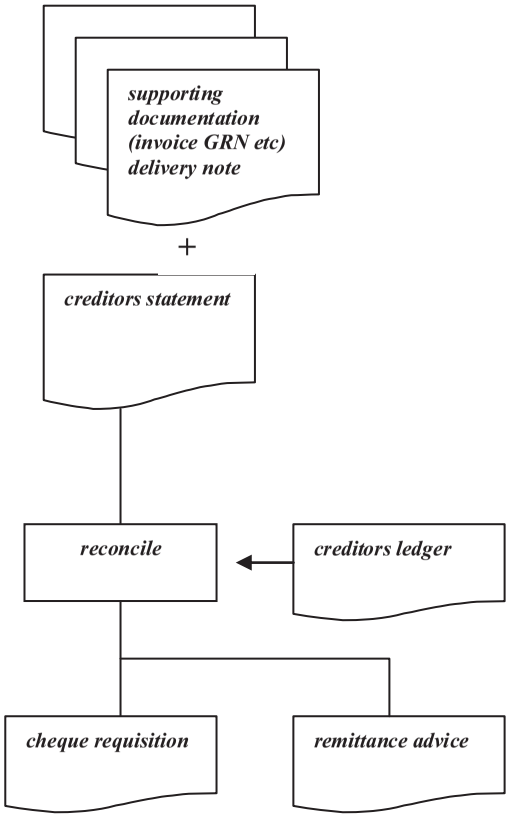
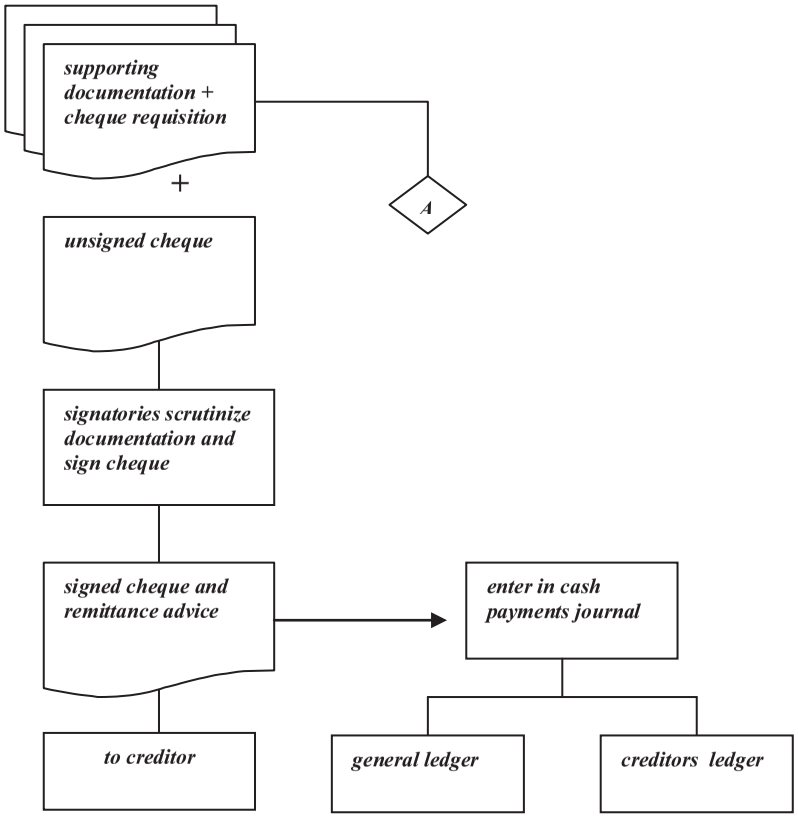
In addition to the above documents, use is made of a ***purchase journal***, ***creditors ledger, the general ledger***, and a ***purchases returns and allowances journal*** to record credit notes and any other adjustments.

In a computerized system, terminology is slightly different, e.g. a goods received note may be referred to as a receiving report, and the creditors ledger will be referred to as the supplier or creditors masterfile.

7. FLOWCHARTS FOR A MANUAL ACQUISITIONS AND PAYMENTS CYCLE

A simple flowchart supported by a series of control activity charts is provided to give you a solid understanding of how a manual system works. As with the other systems, we have assumed that the company has sufficient staff to achieve a clear division between the different functions.


ORDERING
requisition
select supplier source goods
4
3
2
purchase order
1
N
to recording
to receiving
to supplier
RECEIVING
purchase order
2
2
supplier delivery note
1
goods
match goods, order and delivery note
3
2
goods received note
1
N
to recording
to stores with goods
RECORDING OF PURCHASES
suppliers invoice
purchase order
3
goods received note
2
delivery note
match documents, check prices, calculations etc reconcile
enter in purchase journal
general ledger
creditors ledger
Key:
N
= Filed numerically
A
= Filed alphabetically
= document
= action

PAYMENT PREPARATION	*ACTUAL PAYMENT AND RECORDING*
	

ORDERING OF GOODS (AND SERVICES)		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The purpose of this function is to initiate orders so that items/services required to maintain optimum conditions within the organisation, are always available, e.g. manufacturing does not run out of raw materials or parts, or a retailer does not run out of goods to sell. The function is also responsible for placing official orders with suppliers having established that delivery, quality, quantity and price requirements have been satisfied.	Requisition Purchase order form	* ordering of incorrect or unnecessary goods, resulting in liquidity problems and wastage * ordering unauthorised goods resulting in losses to the company through fraud * requisitions not acted upon or orders not placed timeously or at all * obtaining inferior quality goods * paying unnecessarily high prices for goods * orders placed with suppliers not filled / not timeously filled * order forms misused e.g. for placing orders for private purchases

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. order clerks should not place an order without receiving an authorised requisition * the order should be cross referenced to the requisition * prior to the requisition being made out, inventory/production personnel should confirm that the goods are really needed especially where preset re-order levels and re-order quantities are used as the basis for the requisition. 2. before the order is placed, a supervisor/senior buyer should: * check the order to the requisition for accuracy and authority * review the order for suitability of supplier, reasonableness of price and quantity, and nature of goods being ordered (are they items used or sold by the company). 3. the company should preferably have an approved supplier list to which the buyer should refer when ordering * if the company does not have approved suppliers the buyer should seek quotes etc. from a number of suppliers before placing the order * even when ordering from an approved supplier, the buyer should contact the supplier to confirm availability and delivery dates. Note: Before a supplier is approved, senior personnel should carefully evaluate the company in respect of their reliability and the quality and price of its goods. 4. the ordering department should file requisitions sequentially by department (each department will have its own book of requisition forms) and should frequently review the files for requisitions which have not been cross referenced to an order. 5. a copy of the order should be filed sequentially and the file should be sequenced checked and frequently cross referenced to goods received notes, to confirm that goods ordered have been received. Alternatively the pending file of purchase order forms in the receiving bay can be reviewed for orders which are long outstanding. 6. blank order forms should be subject to sound stationery controls. Note: whenever a control procedure is carried out, the employee responsible for the control should sign the relevant document record.

RECEIVING OF GOODS		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The purpose of this function is to accept and acknowledge deliveries of valid orders from suppliers and to record the delivery (goods received note). Prior to acceptance, physical checks on quantity, quality and description of goods should be carried out.	Supplier delivery note (DN) Goods Received Note (GRN)	* acceptance of • short deliveries as full deliveries • damaged and broken items • items not ordered • goods not of the required type or quality * goods received notes not made out accurately or completely * no goods received note made out * theft by employees or outside parties, e.g. collusion with supplier delivery personnel

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS

1. the responsibility for receiving goods should be designated to a goods receiving section which should be physically secured and access controlled

2. on arrival of the delivery vehicle, goods should be offloaded in the presence of a goods receiving clerk who should:
   - 2.1 obtain the supplier delivery note from the delivery personnel and by referring to the order number thereon, locate the purchase order (which should have been filed numerically)
   - 2.2 check the quantity and description of goods delivered against the purchase order and the customer delivery note
   - 2.3 perform at least a superficial test of the condition of the goods delivered e.g. broken or wet boxes.
   - 2.4 reject all incorrect deliveries and clearly identify rejections on both copies of the delivery note and purchase order
   - 2.5 accept goods short delivered but identify such goods clearly on the delivery notes and purchase order (the quantity actually accepted must be clearly identified)
   - 2.6 include on the goods received note, only those goods which have been accepted
   - 2.7 ensure that the suppliers' personnel sign both copies of the delivery note including all amendments e.g. identification of short deliveries
   - 2.8 sign the supplier delivery note

3. on transfer of the goods to the warehouse (custody), the warehouse clerk should compare the physical goods to the goods received note and acknowledge receipt by signing the GRN. Any discrepancies should be reported to the warehouse controller immediately.

Note: Because collusion in this cycle is a major problem for many companies, isolation of responsibilities, sound personnel practices and ***independent*** physical controls should be implemented by ***all*** companies in the supply chain e.g. surveillance cameras, tracing devices on supplier vehicles, should be implemented.

Note: Whenever a control procedure is carried out, the employee responsible for the control should sign the relevant document record.

RECORDING OF PURCHASES		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The purpose of this function is to raise the purchase and the corresponding liability in the accounting records. The recording of ***all*** purchases and trade liabilities should be carried out by the (creditors) recording function so that controls are not bypassed e.g. by the raising of liabilities through the general journal by other departments.	Purchase invoice (PI) Credit Note (CN) Creditors statements Purchases journal Purchases returns & allowances journal Creditors ledger General ledger	* the recording of incorrect amounts arising from incorrect purchase invoices • quantity, quality and type not as ordered or received • prices of goods not as quoted • calculation errors e.g. casts, extentions, VAT * the raising of fictitious purchases/creditors by the introduction of invoices which are for goods never ordered or received by the company. (Results in invalid flows of cash leaving the company). * delays, misallocation and posting errors when entering details into accounting records resulting in reconciliation problems and failure to make use of favourable settlement terms

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. the purchase invoices received from the supplier should be: 1.1 matched to the corresponding goods received note, delivery note and purchase order for: * quantity and description of goods * correct prices and discounts (from order or supplier price lists) 1.2 reviewed to confirm that the amounts on the invoice have been allocated to the correct account e.g. inventory, consumables, stationery. 2. when a requisition is made out to initiate an order, the account to which the purchase must be allocated in the purchase journal should be selected from the "official list of accounts" and entered onto the requisition and then transferred to the order. (If this is not done, the clerk responsible for the allocation of the purchase will not know which account to allocate it to). 3. all casts, extentions and calculations on the invoice should be reperformed. 4. a specific employee should be designated the responsibility of ensuring, by scrutiny of dates of goods received notes and invoices in the pending file, that purchases are timeously and accurately recorded in the purchase journal and correctly posted to the creditors ledger. 5. As the rendering of services by a supplier does not usually result in a GRN, the supplier invoice will normally be signed by the head of the section/department to whom the service was rendered, as proof and approval of the service rendered. Note: whenever a control procedure is carried out, the employee responsible for the control should sign the relevant document record.

PAYMENT PREPARATION (requisitioning)		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The role of this function is to ensure that only valid creditors are paid and that they are paid the correct amount, on time. The function will produce a cheque requisition. The cheque requisition will initiate the preparation of the cheque to be sent to the creditor (see next function).	Remittance advice (RA) Cheque requisition	* payment to fictitious creditors * payment of incorrect amounts * unauthorised payments * discounts lost due to late payment

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. The monthly creditors statement sent by the supplier should be reconciled to the supporting documentation, e.g. invoices, payments etc, and the creditors clerk should ensure that the invoices were subjected to accuracy controls before being recorded. 2. The individual creditor's accounts in the creditors ledger should be reconciled with the monthly creditors statements sent by the suppliers. 3. A creditors clerk should identify those creditors who must be paid at month end to comply with the suppliers' credit terms and to ensure that discounts available for early settlement, are deducted. 4. Cheque requisitions should be sequenced and preprinted and unused requisitions subject to sound stationery controls. 5. Cheque requisitions should include details of the cheque being requested and should be authorized by the preparer of the requisition. (There may also be a review or second authorization procedure by another employee). 6. The cheque requisitions and supporting documentation should be presented to the cheque signatories (simple batch controls may be put in place if cheque requisitions are numerous). Note: whenever a control procedure is carried out, the employee responsible for the control should sign the relevant document record

Note: As previously mentioned, the preferred method of paying creditors is payment by EFT. Paying by EFT does not mean that the controls which must be in place before and after a payment is made e.g. scrutiny of supporting documentation, two individuals to authorize payments and reconciliations and review of cash journals and bank statements subsequent to payment can be ignored; they will be implemented but in another form (this is explained later in the chapter).

ACTUAL PAYMENT (preparing the cheque) AND RECORDING		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The purpose of this function is to produce a valid, accurate and authorised cheque and to record all cheque payments accurately and timeously in the accounting records.	Cheque Returned paid cheque Bank statement Cash payments journal (CPJ) Creditors and general ledger	* cheques may be incorrectly made out (e.g. wrong payee, amount) * invalid payments may be made (e.g. fictitious creditors, overpayments) * payments may be recorded inaccurately (errors) or may be intentionally misstated to hide fraud.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. there should be two cheque signatories for all cheque payments. 2. cheque signatories should agree details on the cheque, i.e. date, amount, payee, to the supporting documentation (invoice, goods received note, remittance advice) 3. cheque signatories should cancel (by stamp or crossing) all documentation so that it cannot be presented again in support of a payment. 4. all cheques should be made out in a manner which makes subsequent tampering with the cheque very difficult e.g. * use of permanent ink * no gaps into which additional detail can be inserted to change the amount or payee * writing out the payee's name in full * crossing cheques "not transferable" 5. cheque books and cheques should be issued in strict numerical sequence and if possible, restricted to only one in issue at any time, and should be subject to strict stationery controls. 6. if a cheque is incorrectly made out, the face of the cheque should be stamped "cancelled" and the signature torn off. The cheque should be retained not thrown away. Note: banks will not accept cheques with alterations due to the high incidence of cheque fraud. 7. signed cheques should not be returned to the preparer but should be mailed by an independent employee. 8. all cheques should be recorded in numerical sequence in the CPJ. 9. the CPJ should be reviewed regularly, by management, for missing cheque numbers and unusual payments. 10. reconciliation of the cash book to the bank statement should be performed and reviewed monthly, by employees who are independent of banking functions, and the creditors department. 11. returned paid cheques should be * filed in numerical sequence * reviewed for suspicious endorsements, payees, amounts by someone independent of the initial preparation of the cheque. This is an additional and simple detection check on the payment system as a whole. Note: whenever a control procedure is carried out, the employee responsible for the control should sign the relevant document record.

8. COMPUTERISATION OF THE ACQUISITIONS AND PAYMENTS CYCLE

Before we deal with the computerisation of this cycle, it will be useful for you to remind yourself of the following points. You can also refer to chapter 8 for a more comprehensive discussion on these points.

8.1 Access.

Many businesses will run their accounting systems on a local area network. Simplistically speaking, this means that there will be a number of terminals, usually from different departments, "linked" together and sharing resources. So access to the network and to individual applications, must be carefully controlled;

- access to the network should only be possible through authorised terminals
- only employees who work in the various functions of the cycle need access to the acquisitions and payments application and only to those modules or functions of the application necessary for them to do their jobs (least privilege/need to know basis). Certain managers will have extensive read only access for supervisory and review purposes.

Various techniques are used to control access. For example, the user

- must ***identify*** himself to the system with a valid user ID
- must ***authenticate*** himself to the system with a valid password
- will only be given access to those programmes and data files to which he is ***authorised*** to have access in terms of his user profile.

Once the user has got onto the system, access is usually controlled by what appears or does not appear on the user's screen. For example, only the modules of the application to which the user has access will appear on the screen, or alternatively, all the modules will be listed, but the ones the user has access to will be highlighted in some way, e.g. a different colour. If the user selects a module to which he does not have access (this is determined by his user profile), nothing will happen and/or a message will appear on the screen which says something like "access denied". In another similar method of controlling access, the screen will not give the user the option to carry out a particular action. For example, certain purchase orders awaiting approval from the chief buyer are listed on a pending file. Although other users may have access to this file for information purposes, when they access the file their screens will either not show an "approve option", or the "approve option" will be shaded and will not react if the user "clicks" on it. Only the chief buyer's screen will have an approve option which can be activated.

Remember that access controls are a very effective way of achieving sound segregation of duties and isolation of responsibilities.

8.2 Menus.

Current software is all menu driven and generally easy to use. Menus can be tailored to the specific needs of a user (based on the user profile) and "items" can be selected by a simple "click of the mouse". Menus facilitate access control and segregation of duties.

8.3 Integration.

The extent to which the accounting system is integrated will vary, but most systems these days are integrated in the sense that a transaction entered onto the system, will instantly update all the records it affects. For example, the processing of a payment to a supplier will simultaneously update the cash records and creditors masterfile. This significantly improves the accuracy of the records ***but*** makes the control over input extremely important.

8.4 Screen aids and programme (automated) checks.

These control techniques which are obviously only available in computerized systems, help ensure that transactions processed actually occurred, were authorised and are accurately and completely recorded and processed. The extent to which these are incorporated into acquisitions and payments applications will vary depending on the quality and cost of the software. These controls are essentially preventive at the input stage and detective thereafter.

8.5 Logs and reports.

A computer can be programmed to produce any number of logs and reports. These can be used as detective controls or for monitoring performance. For example, in the acquisitions and payments cycle, a log of all creditors masterfile amendments should be produced by the computer. This log will be a listing of all amendments that were made, what the amendment was (e.g. creditor's banking details changed) who made the amendment and when it was made. "Read only" access to this file will be given to a senior member in the creditors section so that the amendments made can be confirmed as being authorised, accurate and complete by reference to the masterfile amendment forms. This log can be printed out or accessed on screen. Another example in an acquisitions and payments system would be the production of a report of all purchase orders which are outstanding (e.g. goods have not been delivered). The important point about logs and reports is that unless an employee actually uses them and follows up on any problems, they are worthless. Their huge potential value is that if the logs and report files are properly access protected, they provide ***independent*** evidence of what has taken place on the computer. They form a very important part of the ***audit trail***.

8.6 Matching and minimum entry.

Once data is in the database other data can be "matched" against it. A simple example would be where a creditor's account number is matched against the creditors masterfile to determine whether it is a valid account number. The fact that data is stored in the database also means that the principle of minimum entry can apply. For example, when a goods receiving clerk keys in a purchase order number when receiving a delivery, the full details of the order will appear on the screen. The speed, accuracy and completeness of input is enhanced.

8.7 On system approval.

Where hardcopy documents require approval, it is usually just a matter of presenting the authorising employee with the document and supporting evidence. In a computerised system, approval is frequently given on the system itself and the supporting evidence is also frequently on the system as well. There will be variations on how this is done, depending on the software.

8.8 Audit trail.

An audit trail is a record of the activities which have happened on the system which enables the sequence of events for a transaction to be tracked and examined, from start to finish. It should be possible to identify an invoice raised against a creditor reflected in the general ledger and trace it back to the purchase order placed with the supplier. A system where there is a poor audit trail, will be a weak system. The trail will often be a combination of electronic and hardcopy data.

A NARRATIVE DESCRIPTION OF A COMPUTERISED ACQUISITIONS AND PAYMENTS CYCLE

For the purposes of this illustration, we have described the system for a medium sized wholesale company which purchases its products (toys) from a large selection of local suppliers.

- its accounting systems are integrated
- purchases are only made on credit from approved suppliers
- purchase transactions are processed in real time and all records affected by the purchase are updated instantly, e.g. creditors masterfile, inventory masterfile
- purchase orders are created on screen, approved and then either sent by email or fax to the supplier or the supplier is phoned
- the company is large enough to implement sound segregation of duties with separate departments, i.e. ordering, goods receiving section
- the company has a link to its bank and all creditors are paid by EFT
- creditors are raised at the time the goods are received

The creditors masterfile

The creditors masterfile is central to an acquisition and payments system. The processing of genuine authorized purchases and payments accurately and completely, depends to a great extent on the integrity of this masterfile. The creditors masterfile will contain information which controls which suppliers the company buys from, the terms which affect payments, balances and most important, the banking details required to make EFT payments to the creditors. Access to the masterfile, particularly write access, i.e. the ability to make amendments, must be strictly controlled. Equally important is the control over the amendments themselves to ensure they are authorized and that they are actually processed accurately and completely.

Controls over masterfile amendments will be primarily ***preventive***, but will be supported by detective controls, e.g. checking of logs of amendments. Important amendments to the creditors masterfile will include, adding an approved supplier and changing a creditor's banking details.

Activity/procedure	*Control, comment and explanation*
1. Record all masterfile amendments on a source document.	1.1 ***All*** amendments to be recorded on hardcopy masterfile amendment forms MAFs (no verbal instructions) (see Note (b) on page 11/18). 1.2 MAFs to be pre-printed, sequenced and designed in terms of sound document design principles.
2. Authorise MAF.	2.1 The MAFs should be * signed by two reasonably senior creditors section/accounting personnel (e.g. creditors section head and financial accountant after they have agreed the details of the amendment to the supporting documentation, e.g. MAF checked against the written notification from the supplier that the company's bank account details have changed) * cross referenced to the supporting documentation.
3. Enter only authorised masterfile amendments onto the system accurately and completely.	3.1 Restrict write access to the creditors masterfile to a specific member of the section by the use of user ID and passwords (see Note (a) on page 11/18). 3.2 All masterfile amendments should be automatically logged by the computer on ***sequenced*** logs and there should be ***no write access*** to the logs (this allows subsequent checking of the MAFs entered for authority) 3.3 To enhance the accuracy and completeness of the keying in of masterfile amendments and to ***detect invalid conditions***, screen aids and programme checks can be implemented. ***screen aids and related features*** * minimum keying in of information. For example when amending existing creditors records, the user will only key in the creditor's account number to bring up all the details of the creditor * screen formatting, e.g. screen looks like MAF, screen dialogue * the account number for a new supplier is generated by the system ***programme checks***, e.g. (see Note (c) on page 11/18) * verification/matching checks to validate a creditor's account number

	against the creditors masterfile (invalid account number, no amendment) * alphanumeric checks * data approval check, e.g. must enter either 30 days or 60 days in the payment terms field, not say, 120 days * mandatory/missing data checks, e.g. credit limit and terms must be entered, e.g. account number of creditor ***and*** branch code for the creditor's bank * sequence check on MAFs entered
4. Review masterfile amendments to ensure they occurred, were authorised and were accurately and completely processed.	4.1 The logs should be reviewed regularly by a senior staff member e.g. financial manager 4.2 The sequence of the logs themselves should be checked (for any missing logs) 4.3 Each logged amendment should be checked to confirm that it is supported by a properly authorised MAF and 4.4 That the detail, e.g. the supplier's bank account number, amounts, etc, is correct 4.5 The MAFs themselves should be sequence checked against the log to confirm that all MAFs were entered

Note (a): The authority needed to enter different types of masterfile amendment can be given to different levels of employee e.g. changing a bank account number may be restricted to a single senior employee, but changing an address or contact details could be assigned to a lower level employee.

Note (b): Unused MAFs and other important supporting documentation should be subject to stationery controls as it is more difficult to create an invalid masterfile amendment without the source document.

Note (c): A masterfile amendment should be carefully checked in all respects before it is authorised, so that there should be a minimum of errors or invalid conditions having to be identified (detected) by the programme controls. Each company will decide for itself the extent of programme controls it wishes to implement.

Ordering of goods
A purchase order clerk needs to know what goods to order. How this is done in practice varies, and will depend on the size of the business, the products it sells, or whether there is a manufacturing process. One of the ways in which a requisition for goods to be ordered can be initiated, is by the setting of re-order levels and re-order quantities and then entering them in the inventory masterfile. This means that when the quantity field on the inventory masterfile gets down to a pre-determined level, the system will alert the inventory controller/buying department. There are a number of interrelated activities which make up an acquisitions and payments system and these are described below.

Procedure/activity	*Control, comment and explanation*
1. Setting and protecting re-order levels and re-order quantities recorded in the inventory masterfile.	1.1 These levels should be set by experienced personnel for each item the company purchases and are based on such things as supplier lead times, sales forecasts, average sales over preceding months, etc. 1.2 The pre-set levels should be regularly reviewed. 1.3 The ability to change a level will be restricted to the chief buyer and all changes will be logged. 1.4 Levels will only be used as a guide for determining quantities to be purchased.
2. Initiating a purchase order.	2.1 At regular intervals, say every Monday morning, a purchase requisition report will be generated from the inventory masterfile of items which have reached their re-order levels. The report printed out will contain • the company's inventory code for each item which has reached its re-order level • a brief description of the item • the recommended re-order quantity from the masterfile • a space for the inventory controller to add in any additional comments pertaining to the purchase e.g. changes to the recommended re-order quantity, additional inventory items to be purchased.

	2.2 The report itself should be clearly headed, dated, page sequenced, e.g. page 5 of 5 and clearly laid out. 2.3 The inventory controller should review the report, add comments and meet with the chief buyer to discuss the purchase requisition report before signing it 2.4 Once the chief buyer has reviewed the schedule and added any comments, he should sign it before passing it onto the buying clerk. A copy of the report will be retained by the chief buyer. 2.5 The chief buyer has read access to the creditors masterfile so that for urgent or large orders he can determine whether the account is up to date etc, ***before*** the order is sent to the supplier.
3. Creating a purchase order * purchase orders are made out only for goods that are sold by the company * purchases are only made from approved suppliers * all details pertaining to the order are entered accurately and completely * an appropriate quantity is ordered * all goods on the purchase requisition, and only goods on the purchase requisition report are ordered	3.1 Access to the "create purchase order" module should be restricted to the purchase order clerk. 3.2 On accessing the module, the screen will come up formatted as a purchase order. 3.3 Valid goods: on keying in the inventory item code in the designated field (taken from the requisition report) the description of the goods and the ***supplier's*** inventory item code will appear. If the item code is not a valid inventory code the order clerk will not be able to proceed. 3.4 Approved supplier: when the item code is entered, details of the supplier of the item as listed in the inventory masterfile/creditors' file will appear. The system will not allow the order clerk to enter any supplier who is not approved. The controls in 3.3 and 3.4 can be regarded as ***verification*** checks and are also a form of ***data approval/authorization check***. The entry of the inventory item code to bring up all related inventory details is an example of the ***minimum entry*** principle. 3.5 For accuracy and completeness of entry * the system will automatically insert a purchase order number/reference * alphanumeric check, e.g. on quantity ordered field * mandatory field check on the quantity ordered field and the account to which the purchase order must be allocated, e.g. stores, stationery, security * possible limit or reasonableness check on quantity ordered field, e.g. quantity greater than recommended re-order level on inventory masterfile is not accepted (limit check), or the order clerk is alerted (screen message) if the quantity entered is say, in excess of the average of the last three orders for that item

	* the cost price of the items purchased will be imported onto the purchase order direct from the inventory masterfile 3.6 If the order clerk has any queries pertaining to the goods to be purchased e.g. confirming a price or availability, he will contact the supplier. The order clerk should have read access to the inventory masterfile.
4. Authorising and sending the purchase orders.	4.1 Once the order clerk has compiled the file of purchase orders, it will be available on the system to be accessed by the chief buyer for approval * the approval function will be linked to the chief buyer's user profile * the order clerk will not have approval privileges, e.g. his screen will either have no visible "approve" option for him to select or it will be shaded and will not respond if "clicked" on. 4.2 The chief buyer will access the file of purchase orders (read only) and * check each order against the purchase requisition report for anything unusual, as well as compliance with his instructions if any, relating to the quantity ordered * confirm that there is an order for all the items on the purchase requisition report and that no additional items were ordered. (Note the computer could be programmed to produce a list of all items ordered in the same sequence as the purchase requisition report was produced. Each item would be cross referenced to the relevant purchase order for easy checking.) * the chief buyer should not have write access to the file and changes which he might require e.g. a quantity change, will have to be made by the order clerk and the approval process repeated (segregation of duties) * once the purchase order file has been approved by the chief buyer no changes can be made to the purchase orders file by the purchase order clerk 4.3 Once the approval option is selected by the chief buyer, a message will be sent to the order clerk's terminal alerting him that the purchase orders have been approved. He will then execute the orders either by phoning the supplier, emailing or faxing the order.
5. Maintenance of the inventory masterfile An accurate and up to date ***inventory*** masterfile is absolutely essential for the proper functioning of the purchase order system, as information from the inventory file is used in the preparation of the purchase order.	5.1 Before a new supplier is added to the creditors masterfile/inventory masterfile, a thorough investigation of the supplier should be carried out with regard to pricing, quality of goods and the reliability of the supplier. 5.2 Information about inventory items, e.g. price changes, should be kept up to date

Receiving and recording the goods ordered
This is mainly the physical activity of accepting the goods delivered by the supplier, and recording the receipt of the goods on the system. As the information about the goods being received is already on the system, there is no need to create a goods received note from scratch. We have assumed for the purposes of this illustration, that the supplier invoice is delivered with the goods, accompanied by a delivery note. Remember that the policy should be for the company to receive only goods that are included on the purchase order with regard to description and quantity. The (receiving) company will not want to raise inaccurate supplier invoices on its system, e.g. an invoice for goods which were never ordered or received, or which has been inaccurately compiled.

Activity/procedure	*Control, comment and explanation*
1. Receiving and checking the goods from the supplier.	1.1 Access to the receiving goods module should be restricted to the receiving clerk. On selecting this module the screen will come up formatted as a goods received note. 1.2 Access to the receiving goods module may be restricted to a terminal(s) in the receiving area. 1.3 On arrival of the goods the receiving clerk should access the purchase order file by entering the purchase order number taken from the supplier delivery note • if no number is entered or a number is entered but cannot be matched to a purchase order on the system, the receiving clerk will not be able to proceed • before rejecting the delivery, the receiving clerk will check with the order clerk to confirm that the goods delivered were not ordered. 1.4 The receiving clerk will count the goods and compare what has been delivered to the suppliers delivery note and the purchase order. He should • perform at least a superficial test on the condition of the goods, e.g. reject broken boxes • reject all items delivered which were not ordered in terms of the purchase order • accept goods that have been short delivered in terms of the purchase order • reject any quantities of goods delivered over and above the quantity ordered. 1.5 All discrepancies between what was ordered and what was delivered should be noted on the supplier delivery note. Both the supplier's delivery personnel and

	the receiving clerk should sign the documentation to acknowledge the discrepancies. 1.6 The receiving clerk will have write access to only the quantity field on the GRN. Confirmation of the GRN (once any corrections have been made to quantities) will update the inventory masterfile. 1.7 A copy of the GRN will be printed out to accompany the goods to the custody section of the warehouse and the supplier delivery note and invoice will be sent to the accounting department. The accounting department will be able to access the GRN on the system.
2. Recording the purchase and corresponding liability in the records	2.1 Recording of the supplier's invoice in the accounting department (not in receiving). 2.2 Access to the raising invoice module will be restricted to the creditors clerk. 2.3 The creditors clerk should access the purchase order file by entering the purchase order number relevant to the supplier invoice (this number should be on the invoice). An incorrect or non-existent number will be rejected. 2.4 On the entry of a valid purchase order number, the screen will come up formatted as an invoice. This on-screen "document" will reflect the exact details of the applicable purchase order, e.g. supplier details, description of goods, cost and quantity of goods ordered. Where necessary the quantity ordered would have been adjusted at the time the goods were received. 2.5 The creditors clerk should compare the details on the screen to the hardcopy invoice and supplier delivery note and confirm that • only goods which were ordered were received (receiving clerk should have rejected goods not on the purchase order) • the quantity ordered, received and invoiced reconcile with each other • prices on the supplier invoice are correct in terms of the purchase order • casts, extentions and VAT are correct. 2.6 If a price differs between the purchase order and the supplier invoice, the creditors clerk should contact the supplier and the order clerk to confirm the correct price. Note, the objective is to raise the correct amount owed in respect of what was received. 2.7 The system will prevent the creditors clerk from adding additional items onto the invoice. 2.8 All changes, e.g. to cost prices, will be logged and followed up. 2.9 The on-screen supplier invoice should be approved by a second creditors clerk.

	2.10 On selecting the confirm/accept option, the file of invoices and the creditors masterfile will be updated (the liability has been raised). 2.11 On a weekly basis, a report should be run of all GRNs for which a supplier invoice has not been received, e.g. the goods have been delivered but the invoice has not been sent or has been lost.

Payment of creditors by electronic funds transfer

As discussed in chapter 9, electronic funds transfer is a very fast and efficient method of making payments, but it is perhaps for these very reasons that the risk of fraudulent payments (theft of funds from the company's bank account) will be very high if strict controls are not in place. The controls over EFT payments will centre around:

* controlling access to the creditors masterfile. It should not be possible to add a fictitious creditor to whom fictitious payments can be made, and it should not be possible to alter an existing creditor's banking details other than under strictly controlled conditions
* approving details and amounts to be paid to the creditor
* controlling access to the company's bank account
* reviewing EFT payments actually made promptly.

We have assumed, for the purposes of this illustration, that creditors are paid monthly and payments are made on the strength of unpaid invoices listed on the system, i.e. the company does not wait for a statement from the creditor. Creditors reconciliations (between suppliers statement and the creditors' account in the masterfile) will take place at a later stage.

Activity/procedure	*Control, comment and explanation*
1. Preparation of the schedule of payments How the schedule is actually compiled will depend on the software. The objective is to prepare an accurate and complete schedule of amounts actually owed and due for payment.	1.1 The preparation of the EFT schedule of payments to creditors and the authorization thereof will be carried out by different employees • the creditors clerk will prepare the schedule • the head of the creditors section will authorize it 1.2 As all the information to prepare the schedule is already on the system, the software will be designed to minimize the need to enter any additional information. This enhances accuracy and completeness and prevents the addition of fictitious payments.

	1.3 Write access to the "prepare payment module" will be restricted to the creditors clerk preparing the schedule. 1.4 Once the module has been entered, the creditors clerk will either select a creditor by clicking on the list of creditors which appears on the screen, or alternatively the screen will automatically display the first creditor in alphabetic order • the screen will be formatted as a payment document which will reflect the creditors standing data • on selecting the "select invoices" option, a dropdown list of all unpaid invoices for that creditor will appear (remember that a file of all unpaid invoices is already on the system) • the creditors clerk will select those invoices which the company should pay, governed by the terms agreed with the creditor, e.g. 30 days. The creditors clerk will have a facility which enables him to call up supporting documentation on the screen or he may choose to inspect hard copy. This procedure will be followed for each creditor and as each payment document is completed it will be listed on the payments schedule • if there is nothing to be paid to a creditor, the creditor will still be listed but the amount to be paid will be nil • a financial total of all amounts to be paid to creditors will be computed and there may be a processing control which compares this total with the amount by which the total on the unpaid invoices file has been reduced • as the invoices are selected for payment, they will be removed from the file of unpaid invoices or a status code will automatically be attached to indicate that the invoice has been paid. This also ensures that it cannot be selected for payment again. 1.5 Once the schedule has been prepared, the creditors clerk will select the proceed option and at this point the file can no longer be altered. The creditors clerk will not have an approve option on his screen.
2. Approval of the schedule of payments	2.1 To approve the schedule of payments, the creditors section head will access the schedule of payments file. He will have read access only. He should • review the schedule for reasonableness, looking for any payments which appear abnormal, e.g. large amounts, or regular suppliers for whom there is no payment amount. • run reports to assist him in his review, e.g. o report of creditors which are on the current months schedule but were

	not on the previous month's schedule. These will be confirmed against the log of masterfile amendments as they should represent new creditors put onto the masterfile o a report (log) of all amendments to creditors bank details. He should verify these against the masterfile amendment form and supporting evidence supplied by the creditor and possibly even confirm the change directly with the creditor o a report which provides comparison of amounts paid to each creditor for each of the previous three months o a report of any discounts taken to ensure that the discount is valid and correctly computed and that any discounts to which the company is entitled have been taken o make use of the facility which enables him to bring up on screen, copies of the relevant purchase order, GRN and invoice to confirm details of amounts owed. He may also refer to hardcopy documentation. 2.2 The head of the creditors section should not have write access to the payment schedule file. Any changes he may require will be referred back to the creditors clerk. 2.3 Approval of the payments schedule will be on screen (on the system) and the ability to approve the file will be restricted to the section head. Note: There is nothing to stop the schedule of payments from being printed out for detailed checking and authorization. If this is the case it will be approved by signature and will need to be agreed to the schedule on the system before the EFT is effected.
3. Access to the bank account on the internet	3.1 The bank's EFT software will be loaded on a limited number of the company's terminals. 3.2 Access to the bank's site on the web will be gained in the normal manner but once the employee gets onto the site an additional PIN number supplied by the bank and a password, unique to the employee will have to be entered to gain access to the company's account • the privilege to access the company's account will only be granted to employees who need access to the bank account to carry out their duties. 3.3 If this identification and authentication process is accepted, a menu of the functions available to the company will appear on the screen, e.g. balance enquiry, payment query, download bank statement, make EFT payment. 3.4 Access to these functions will be directly linked to the employee's user profile on a need to know basis. The function which needs to be most protected will be

	the ability to make an EFT payment • this privilege will be granted to a limited number of senior personnel (much like giving senior employees cheque signing powers) • an additional ***authentication*** procedure will be required, e.g. an additional one time password or the insertion of a physical device into the USB port of a terminal on which the bank's software is loaded (see chapter 9/19 for a discussion on these devices)
4. Approving (effecting) the payment We will assume for the purposes of this illustration, that the company's bank requires an additional one-time password to be entered and that to generate the number, each employee authorized to effect an EFT is given a device to generate the random number. We will also assume that the creditor's section head and two other senior officials have this privilege.	4.1 At least two of the three authorized employees will be required to effect the payment of creditors, e.g. the creditors section head will authorize the payment and the financial manager will release it by the entry of their one-time passwords provided by the random number generator. 4.2 Once the head of the creditors section is satisfied with the payment schedule he will select the "first confirmation" option and a system generated message will be sent to the financial manager (second signatory) informing him that the file of payments is awaiting his approval. 4.3 The financial manager will then access the file of payments and carry out whatever procedures he deems necessary to be in a position to authorize the payments, e.g. review of reasonableness, access of masterfile amendment logs, reference to original documentation. * the "second signatory" (financial manager) will also ***not*** have ***write*** access to the file so cannot for example, add a payment * once the "second signatory" is satisfied he will click on "second confirmation". * the second confirmation cannot be activated before the first confirmation. 4.4 The file of payments will now be fully approved, and the clicking on the second confirmation will automatically convert the file to a format compatible with the bank's EFT software. 4.5 Once this has been done, the creditors section head will click on the ***authorize*** option (one time password will be entered) and the financial manager will click on the ***release*** option (one time password will be entered). * the ***release*** activity cannot be activated before the ***authorize*** option. 4.6 Additional controls which should be implemented are * automatic shutdown after three unsuccessful attempts to access the company's bank account on the system * logging of attempts at unauthorized access (successful attempts will also be automatically logged) * the number of bank accounts to which transfers to other bank accounts from the ***main*** bank account should be limited to protect the main bank

	account. For the payment of creditors, an amount equal to the total of individual payments to creditors should be transferred to a second account and the actual transfer to creditors bank accounts should be made from the second account. Transfers to creditors could be scheduled only to take place on a specified date * a limit on the total amount which can be transferred within a 24 hour period can be arranged with the bank as well as a limit on individual payments * data should be encrypted * conventional password controls will apply and physical authentication devices must be kept safe and secure at all times. 4.7 The electronic funds transfer will update the creditors masterfile, cash payments journal and general ledger.
5. Detection of unauthorized payments	5.1 Within a day or two of making the electronic funds transfer, (EFT) the accountant (or similar level employee) should download a copy of the bank statement for the creditors account and compare it to the schedule of payments to creditors.

Processing controls

As mentioned in chapter 8, the accuracy, completeness etc, of processing, are evidenced by reconciliation of output with input and the detailed checking and review of output by users, on the basis that if input and output can be reconciled and checks and reviews reveal no errors, processing was carried out accurately and completely and only transactions which actually occurred and were authorised, were processed. To make sure it does its job, the computer will perform some internal processing controls on itself, but the user will not even be aware that these are going on. The users within the cycle make use of the logs and reports which are produced relating to their functions, whilst the IT systems personnel make sure that processing aspects of the system are operating properly.

Summary

The description of the system described above, provides an illustration of how the control activities described in chapter 5 (and referred to in ISA 315 (Revised)), can be implemented. It also provides an illustration of how specific automated (programme) controls can be introduced. For example:

Segregation of duties	* Separation of functions, e.g. ordering, receiving goods, processing payments. * Separation of responsibilities within functions, e.g. generating purchase requisition report, initiating purchase orders, authorising purchase orders.
Isolation of responsibilities	* Isolating responsibilities through granting access privileges, e.g. only chief buyer can approve purchase orders. * The goods receiving clerk signs the supplier delivery note which isolates his responsibility for accepting the delivery of goods from a supplier.
Approval and authorisation	* The system will not allow the order clerk to place an order with a supplier who is not on the creditors masterfile. * The creditors section head approves the schedule of EFT payments to creditors.
Custody	* Access to the bank account (custody of the company's money) is strictly controlled by user IDs, PINs and passwords (those with authority to make an EFT are effectively the custodians of the company's cash). * Goods received by the goods receiving section are kept securely until they are transferred to the warehouse.
Access controls	* All users on the system must identify and authenticate themselves by IDs and passwords and what they are authorised to do is reflected in their user profiles. * Additional access controls such as terminal shut down and logging of access violations are in place.
Comparison and reconciliation	* The system reconciles the total amount (and number) of invoices selected for payment with the reduction in the total and number of invoices on the unpaid invoices list. * The creditors clerk reconciles the supplier's statement with the creditor's (supplier's) account in the creditors masterfile.

Performance review	* Supervisory and management staff can access the purchase order file to see how efficiently approved purchase orders are being executed. * Reports on inventory ageing (number of days inventory items are held) can give an indication of the appropriateness of re-order levels and the performance of the chief buyer and inventory controller. * Monitoring complaints from the sales manager relating to sales lost because of inefficient purchasing.
Control techniques and application controls	* Screen aids and related features • minimum entry : keying in the inventory code of an item on the purchase order brings up the supplier, description, cost, etc of that inventory item • screen formatting : purchase order • mandatory fields : branch code for new customer banking details. * Programme checks • validation check on supplier number • limit checks/reasonableness checks on quantity ordered field. * Output control • masterfile amendment logs are checked against source documents • bank statement checked against EFT payments entered onto the system.
Logs and reports	* Log of and changes to existing creditors banking details * Weekly reports of long outstanding purchase orders or of GRNs for which there is no invoice.

This does not cover every control, policy or procedure that could be in place and is not intended to. This knowledge will only be acquired when you go into different companies and work with their systems

9. THE ROLE OF THE OTHER COMPONENTS OF INTERNAL CONTROL IN THE ACQUISITIONS AND PAYMENTS CYCLE

This chapter has concentrated on the accounting system which is part of the ***information system*** and ***control activities*** components of internal control. However, these components are affected by the other components, so a brief mention of the role of the other components is necessary.

9.1 The control environment.

The control environment within the cycle will be directly influenced by the control consciousness of the company as a whole. With regard to this cycle specifically, the tone will be set by the actions and control awareness of the chief buyer, the head of the creditors section and the senior employees responsible for the authorization of payments to creditors. There should be strict policies in place relative to the acceptance of inducements from suppliers to purchase their goods such as gifts from suppliers, kickbacks and bribes, but if the chief buyer, or other senior personnel, show little regard for these restrictions, the control environment will deteriorate quickly. Unfortunately this type of practice is widespread.

The other function which must be surrounded by a strong control environment is the payment of creditors. As mentioned earlier, this part of the cycle provides a legitimate process for getting money out of the business, so if controls are not strictly enforced, fraud and theft will surely follow.

Practices such as signatories pre-signing a batch of cheques because they are going to be away, disclosing of passwords for "authorizing" and "release" of EFT payments should not occur under any circumstances.

In a smaller entity there should be comprehensive owner/management involvement in the cycle as it is a cycle very vulnerable to theft.

9.2 Risk assessment process.

The company's formal risk assessment process will address the major risks that face the company and which may have a direct effect on this cycle, e.g. purchasing decisions, such as import or buy local, the need for alternative sources of supply, the social/environmental reputation of the supplier, bribery and kickbacks, and information technology risk (EFT) will be dealt with formally.

Less formal risk assessment can occur within the section by members of the section regularly evaluating the risks and responses already in place to address the specific risks facing the section, e.g. better re-order levels to reduce overstocking, theft of deliveries from suppliers at the receiving stage, etc.

Again in a smaller entity it will be the owner/manager's informal, but ongoing assessment of risk which will be important.

9.3 Monitoring.

How is the cycle doing over time in meeting its objectives? That is the question which monitoring seeks to answer. To express these objectives simplistically, we might describe them as, ensuring optimal quantities of inventory are held, costs of items purchased is as budgeted, suppliers are reliable and that only valid creditors are paid accurately and on time. These can all be monitored by period based comparisons (and industry comparisons, if available) of such matters as

* delays in production or sales lost because of inappropriate inventory holdings
* instances of the inability of suppliers to supply goods as required (price, time and quality)
* actual purchase costs compared to budgeted costs
* complaints from suppliers or letters from suppliers demanding payment
* losses from cheque fraud or EFT fraud
* reductions in theft of inventory.

Monitoring can be carried out by the board through the scrutiny of reports on the above matters or by visits from an internal audit team. Owner/managers pretty much monitor internal control themselves and may do it very well, particularly if they are very involved in the day to day running of the business.

THE ACQUISITIONS AND PAYMENTS CYCLE AT PRORIDE (PTY) LTD

1. INTRODUCTION

At ProRide (Pty) Ltd the acquisitions and payments cycle is taken very seriously. The basic principle (which is followed in all cycles) is that if the initiation of the transactions in the cycle is carefully controlled, then problems arising later in the cycle are kept to a minimum. As you will see, the two most senior members of staff (the managing director and the financial director) are closely involved in initiating and authorising purchase transactions.

Both the managing director (Peter Hutton) and the financial director (Brandon Nel) have extensive knowledge of the bicycle industry. Great care is taken to ensure that inventory of the required quality, price and saleability is obtained. There are two major reasons for this. Firstly, ProRide (Pty) Ltd's largest customers are the major chainstores, and failure to deliver the right product, at the right price, on time, will result in the loss of an important market. Secondly, the company does not want to purchase inventory that it cannot sell.

2. SUPPLIERS

Each and every supplier to ProRide (Pty) Ltd is carefully evaluated by Peter Hutton and Brandon Nel. They require suppliers who are ***reliable with regard to delivery***, who are ***consistent with quality*** and ***who are reasonable with price.*** Suppliers are evaluated on an ongoing basis and a sound business relationship is built up with them. This evaluation includes regular visits to the suppliers premises, a number of whom are as far afield as Taiwan and China.

Prices for each inventory item are negotiated and agreed with local and foreign suppliers, usually for the following six months.

3. PURCHASES

As indicated in Chapter 10, ProRide (Pty) Ltd wholesales bicycles and related spares and accessories. In addition to goods purchased for resale, the company like any other company, purchases other items such as stationery, consumables, minor tools and equipment etc. Whilst these "non trading" items are also subject to sound internal controls, they are not the concern of the two directors.

Purchases are made from both local and overseas suppliers. The basic controls over purchases from both sources are the same. However, in respect of imported purchases, additional procedures arise as goods have to be shipped in containers, and must be cleared through customs etc, before being delivered. Payments to foreign suppliers must be subjected to foreign exchange regulations. Foreign purchases far exceed local purchases.

4. FREQUENCY OF ORDERS

ProRide (Pty) Ltd does not place a huge number of orders. The goods they purchase are obtained from a limited number of suppliers, who between them, supply the full range of ProRide (Pty) Ltd's inventory. To make purchases from foreign suppliers is a reasonably time consuming exercise with long lead times due to the fact that the goods are shipped to South Africa by sea in containers. Clearance through customs also takes time . The result is that large orders are placed with foreign suppliers, usually at about six weekly intervals. Because of this ProRide (Pty) Ltd does not have a separate order department staffed by a chief buyer and a number of buying clerks as it is not necessary. However, the company does have a purchases manager (Ruth Taylor) and she is assisted by Zodwa Mashego and Tania Koetzee, the purchase clerks.

5. COMPUTERISATION

As indicated in Chapter 9, the company uses JD Edwards application software run on an IBM AS 400 system. However, ProRide (Pty) Ltd has ***not*** integrated its acquisitions and payments cycle into this system as the number of purchases made does not warrant the cost of integration. (You will recall from the discussion in Chapter 10 that the cashbook function is not integrated for the same reason).

ACQUISITIONS - HOW THE SYSTEM WORKS

1. INITIATING ORDERS

1.1 Minimum inventory levels/reorder quantities

As explained in Chapter 10, a computerised, real time, perpetual inventory system is maintained. Each inventory item on the inventory masterfile has preset minimum inventory level and re-order quantity fields. These two fields are set by the financial director and the managing director after careful analysis of sales trends, supplier lead times, customer needs etc. The levels are adjusted as conditions change.

Any changes to these fields are treated as masterfile amendments and are subjected to normal masterfile amendment controls. Only Dalene Burger (accounting supervisor) and Gary Powell (IT manager) have the necessary access privileges. Changes must be supported by documentation authorised by Brandon Nel (financial director) and Peter Hutton (managing director). Adjustments are logged by the computer and the logs subsequently reviewed by Brandon Nel.

1.2 Inventory order reports

Once a week a sequenced and dated printout called an ***inventory order report***, is produced. This lists all the inventory items which have reached their preset minimum inventory levels. The list provides the item code, description, supplier details, quantity on hand, cost price and re-order quantity. There is one report for local suppliers and one for foreign suppliers. The foreign supplier report is also analysed by ***supplier name*** e.g. Speedybikes Inc, ***supplier region***, e.g. Taiwan and ***inventory category*** e.g. bicycles. The reason for this will be explained below. An item which has reached its minimum inventory balance will continue to appear on the weekly inventory order report until an order for the item is placed and the order is captured onto the AS 400 system (see 2.3 and 3.3 below).

Because an item appears on the "inventory order report", does not mean that an order is automatically placed. The reports are first given to Brandon Nel (financial director) and Peter Hutton (managing director) for extensive analysis before the decisions about what to order and how many to order are taken. Before they decide on what to order they will again consider factors such as past and future sales trends, the intentions of their major customers, whether the particular item is sufficiently profitable as well as expected lead times and other supplier conditions. This is why their knowledge of the industry is so important. Essentially the inventory order report is simply an indictor that inventory may be required.

2. PURCHASES FROM LOCAL SUPPLIERS

2.1 Frequency

As it is far less complicated and time consuming than ordering daily, purchases from local suppliers are placed weekly. Once Brandon Nel and Peter Hutton have decided what is to be ordered, they place the quantity to be ordered in the blank box provided next to each item on the ***inventory order report*** for local suppliers. If an item is not required, nil is written into the box. Both parties sign the inventory order report and pass it to Zodwa Mashego (purchases clerk). The signed inventory order report is in effect, an inventory requisition.

2.2 Purchase orders

Using a very simple in house programme, resident on her computer, Zodwa captures the details off the signed inventory order report to create a purchase order (PO) two copies of which are printed out. Access to the purchase order software is restricted to Zodwa and Ruth Taylor (purchases manager) using conventional access controls. The principle of minimum entry applies so Zodwa does not have to

capture supplier details etc, or details of the items to be ordered, i.e. entry of the supplier name or account number will bring up the supplier details, and the entry of the item code will bring up the description of the item. (This detail is on the inventory order report from which Zodwa is capturing). The PO is sequenced and dated and Zodwa cross-references it to the inventory order report. The details on the PO captured by Zodwa are then checked against the inventory order report by Tania Koetzee, the other purchases clerk, who signs to acknowledge the procedure.

The PO is then emailed to the supplier. (Note: a single inventory order report will usually result in orders being placed with more than one supplier).

2.3 Entry onto the AS 400

At this point Zodwa Mashego enters the details off each purchase order onto the AS 400 system where it is stored in the ***inventory orders placed*** file. A hardcopy of the file is printed out, checked carefully to the purchase orders by Tania Koetzee the other purchases clerk, and signed by both clerks to be filed with a copy of the PO and the relevant inventory report. No updating of any files on the system takes place e.g. no changes are made to the inventory masterfile. The information is placed on the system for information purposes only . For example Reg Gaard (warehouse manager) can access the system at any time to see what orders he can expect to be delivered, and when the delivery arrives, to confirm what he is receiving is correct in terms of the purchase order. Brandon Nel and Peter Hutton can also follow up on orders by using their enquiry privilege.

3. PURCHASES FROM FOREIGN SUPPLIERS

3.1 Frequency

Foreign purchases are far more complicated. You will recall that the foreign inventory order report is analysed by supplier, supplier region and inventory category. This enables Brandon Nel and Peter Hutton to order in a more efficient manner. Goods are sent by sea in large containers, and it is very expensive and inefficient if the container is not full. It is also impractical and expensive to place lots of orders (for small quantities) with a supplier. Therefore in placing an order Brandon and Peter will attempt to fill a container. Having the inventory order report analysed by ***supplier, region*** and ***inventory category*** (which is broken down into different items) assists in the following way.

supplier : ***all*** goods to be ordered from that supplier are identified. If only a few items are required from a particular supplier, the directors may decide to postpone the ordering of those particular items until a large order can be placed.

supplier region : ***all*** goods from suppliers in Taiwan are identified. This gives the directors an idea of whether it would be efficient to order additional items from other Taiwanese suppliers to fill a container.

inventory category and inventory items : this provides an indication of which categories and items within the category are selling. For example, if it appears that mountain bikes are selling faster than road bicycles then additional mountain bikes may be purchased.

The point that we are trying to illustrate here is that preset ***minimum inventory levels*** and ***re-order quantities*** are used only as indicators, they do not result in an order being automatically generated and sent to a supplier.

3.2 The master form

Once Peter Hutton and Brandon Nel have decided what is to be ordered, the foreign inventory order reports are amended, signed by both of them, and passed to Zodwa Mashego. Using her computer and inhouse developed software, she calls up on screen, a "Master Form" (MF). Each foreign supplier's details are stored on her computer, and once she keys in the name of the supplier a blank MF for that supplier, indicating contact details, terms and a sequence number appears. Zodwa Mashego enters all the details of what is to be ordered from the foreign inventory order report onto the MF. The MF is printed out in duplicate and passed to Tania Koetsee who checks it for accuracy and completeness

against the foreign inventory order report. The Master Form is then passed to Ruth Taylor (purchases manager) who authorises it. The MF is stamped with a grid stamp to facilitate this process as follows.

Prepared by	
Checked by	
Authorised by	

3.3 Contacting the supplier

A copy of the Master Form is then emailed or faxed to the foreign supplier and a pro-forma invoice is requested. The pro-forma invoice is

* an acceptance of the order by the supplier
* a document which can be used for preliminary planning by the shipping agents who clear ProRide (Pty) Ltd's imports through customs and warehousing
* sometimes required by the bank when finance is being arranged.

When the pro-forma invoice is received it is checked again for accuracy and completeness to the "Master Form" by Ruth Taylor who signs it to acknowledge the check.

The signed copy of the pro-forma invoice is passed to Zodwa Mashego (purchases clerk) for entry onto the AS 400 system. As with the entry of local purchases, ***no updating of any accounting records takes place***, the purchase details are placed on the system for information purposes, e.g. planning warehouse space to receive goods, or for Peter Hutton and Brandon Nel to obtain information about outstanding orders.

3.4 Obtaining confirmation that ProRide (Pty) Ltd can pay

Purchasing from foreign suppliers raises two specific issues with regard to payment.

* foreign suppliers are most unlikely to ship the goods before they are satisfied that ProRide (Pty) Ltd will pay
* the payment to foreign suppliers is controlled by ProRide (Pty) Ltd's bank to comply with foreign exchange legislation.

These issues are addressed as follows. Johan Els (financial manager) arranges a Letter of Credit (LC) through Standard Bank, ProRide (Pty) Ltd's bankers. A Letter of Credit is a credit facility in terms of which ProRide (Pty) Ltd agrees to pay the supplier's bank once certain conditions have been met, for example, all shipping and custom documentation has been authorised and submitted to the bank.

Obviously Standard Bank will not issue a Letter of Credit unless they are satisfied with ProRide (Pty) Ltd's creditworthiness. Being the company's bankers they will assess this on an ongoing basis.

Once the LC has been authorised and issued by the bank

* it is attached to the relevant pro-forma invoice from the supplier
* the supplier is notified by email of the details of the Letter of Credit.

3.5 The LC Payment Register

Using the pro-forma invoice and corresponding Letter of Credit, Ruth Taylor writes up (manually) the LC Payment Register. This is, in effect, a foreign creditors ledger, as it shows the amounts owed to the foreign creditors.

3.6 Shipping the goods

Once notified about the Letter of Credit, the supplier will confirm with its bank that the LC is valid, and if it is, will ship the goods and send the following documents to ProRide (Pty) Ltd. These documents are termed the "non negotiable documents" and are sent in duplicate.

* ***Bill of Lading*** : a document signed by the shipping agent which evidences the receipt of the goods on board.
* ***Packing list*** : a document which indicates the total number and type of packages, weights and contents of the shipment.
* ***Final invoice***.

* ***Shipping files***
At this stage a (physical) shipping file is opened for each order . The file is very important as it will become the final destination of all the documents and will provide a comprehensive audit trail for each foreign order. Thus a ***completed*** shipping file will contain
- Foreign inventory order report
- Master Form
- Pro-forma invoice
- Letter of Credit
- Bill of Lading
- Packing list
- Final Invoice
- Any other correspondence
- Goods Received Note) added once the goods have been cleared and delivered
- Clearing Agents documents)

3.7 Forwarding and clearing (shipping)

All imported goods have to be shipped from their country of origin and cleared through customs when they arrive in South Africa. Both of these activities require specialist knowledge due to the complicated nature of the laws and regulations pertaining to importing. It is therefore usual that importers in South Africa make use of agents to assist them; namely, ***forwarding agents*** who control and administer the shipping of the goods, and ***clearing agents*** who guide the goods through customs. To simplify matters ProRide (Pty) Ltd deals directly with one company which offers both these services i.e. forwarding and clearing. We will refer to this company as ProRide (Pty) Ltd's "shipping agents".

Once received, the "non negotiable documents" are passed to Ruth Taylor who files the duplicates and sends the original documents to ProRide (Pty) Ltd's shipping agents. (She also includes a standardised clearing document which give precise details of what is being imported.)

The shipping agent will make payments on ProRide (Pty) Ltd's behalf for various forwarding (shipping) costs as well as clearing costs, such as harbour fees (wharfage), duties and levies. Once the goods have been cleared through customs these costs are recovered from ProRide (Pty) Ltd by the shipping agents and a fee is charged. Like any other local supplier, the shipping agent will send an invoice and documentary evidence of the payments they have made on ProRide (Pty) Ltd's behalf, e.g. forwarding agent's fee, the Portnet invoice for wharfage. Before submitting the invoice to Tania Koetzee for it to be included on the creditors payment schedule (see 7.2 below), Ruth Taylor scrutinizes the invoice and supporting documentation to ensure that all charges are valid, accurate and complete. She then signs the invoice to acknowledge this control procedure.

3.8 The container schedule

Once the "non negotiable documents" are to hand, Ruth Taylor also prepares a hardcopy "container" schedule. This schedule is sent, with a copy of the Packing List to Reg Gaard (warehouse manager) to assist him in scheduling the receiving of the purchases and preparing the warehouse. The schedule contains the following details:

* Ship name and estimated date of arrival
* Container number
* Shipping file number
* Master Form (order) number
* Supplier names

4. RECEIVING THE GOODS

4.1 Supervision

All goods, whether they are local or imported are received in the receiving depot , a physically secure area in the warehouse (see diagram in chapter 12). As explained in chapter 12, the frequency of deliveries does not warrant the appointment of a "specialist" receiving clerk and the responsibility is given to the dispatch clerk and his assistants. Receiving is always supervised by either Reg Gaard or

Patrick Adams the warehouse manager and foreman, respectively. This improves the efficiency of receiving and reduces the incidence of theft before the goods arrive in the warehouse.

4.2 The receiving procedure

Local goods are usually delivered in cartons or boxes by a road delivery service and generally it is impractical to check each item received against the purchase order as the delivery service is keen to get away to make the next delivery. Therefore, the receiving procedure is broken down into two functions. The initial function is taking delivery of the number of cartons/packages from the freight company. The "receiving clerk" will match the description and labeling on the cartons and the delivery company's waybill, and sign the waybill to acknowledge what has been received. If there are any discrepancies, the receiving clerk and the driver will mark the discrepancy on the waybill. A copy of the waybill is retained by the receiving clerk. Imported goods are delivered in containers and a similar process is followed. Because it is not possible, with the large orders received in the container, to check that each item ordered has been received, the first function again is to offload the packages/cartons from the container and compare these to the description of the packages/cartons on the Packing List. Remember that the Packing List describes the number, type and weight of the packages/cartons included in the shipment. Once this "broad" check has been done, Patrick or Reg (who supervise the receipt of imported goods closely) will sign the freight company's delivery note. This is simply an acknowledgement that the packages/cartons which were shipped have been received. The contents have not, at this stage, been checked. A copy of the freight company's delivery note is retained.

All cartons or packages (local and imported) are retained in the receiving area and promptly unpacked for detailed checking against the purchase order/GRN. The process is as follows

* the "receiving clerk" will enter the purchase order number onto the system. If there is a match to the inventory orders placed file (there usually is), the purchase order will come up as a GRN on the screen, and two copies of the GRN (populated with all of the detail of the goods on the purchase order) will be printed out.
* the goods delivered are then carefully checked against the GRN (twice).
* goods that have been delivered incorrectly, e.g. have not been ordered or have been over-delivered, are ***not*** taken into inventory and are stored in a secure area in the receiving section, with a discrepancy report for subsequent return to the supplier.
* discrepancy reports are preprinted and sequenced. When a discrepancy report is completed, full details of the discrepancy are recorded, it is cross-referenced to the purchase order and signed by two individuals, usually the "receiving clerk" and either Reg Gaard or Patrick Adams.
* where necessary, hard copy GRNs and the on-screen GRNs are amended to reflect the ***quantities*** actually received. Changes to the descriptions of goods delivered are not made and no additions of goods delivered but not ordered, are entered. The final GRN must reflect the actual quantities of goods received and only goods on the purchase order. The only field which can be altered on the on-screen GRN is the quantity field and no additional items can be added.
* Reg Gaard (warehouse manager) will confirm that the on-screen GRNs and the hardcopy GRNs agree exactly and he and the receiving clerk will sign the hardcopy.
* once Reg Gaard is satisfied with the on-screen GRN, he will select the "confirm" option and
  - the purchase order on the "inventory orders placed" file will be coded to indicate that the "purchase order" is no longer outstanding
  - the quantity field in the inventory masterfile will be updated.

5. COSTING THE INVENTORY

5.1 When the GRNs arrive in the purchasing department, each inventory item must be costed. This is done as soon as all documents are available. For local purchases the cost is taken off the purchase order. For imported goods a costing exercise to establish the true cost of "bringing the inventory to its location" must be carried out.

The exercise is carried out by Zodwa Mashego or Tania Koetzee (purchases clerks) on a pre-designed costing spreadsheet using Excel software.

An example of the Costing Schedule used by the company is shown below. We will assume that the shipment consisted of 400 Raleigh RC bicycles.

ProRide (Pty) Ltd	***Costing Schedule***	***Date 9 Sept***
Supplier Shimlee Taiwan	***File No***. 702 Shim ***Invoice No*** 1237	
Value per Suppliers Invoice		US$135507
At conversion rate x R10 (note 1)		R1 355 070
Custom clearing charges		6 580
Freight		28 645
Cartage		2 555
Bank charges and fees		840
Total cost		R1 393 690
Cost per unit: Raleigh RC: 400 units		R 3 484 (rounded)
Prepared by:		Checked by:

The preparer signs the schedule and Ruth Taylor checks the costing from the supporting documentation and also signs it. It is then placed in the Shipping File.

Note 1: ProRide (Pty) Ltd buys forward cover to pay for its foreign purchases and complies with the International Accounting Standards when selecting the appropriate conversion rate for costing the inventory.

Note 2: If the shipment contains a number of different items (which is usually the case) the total cost is allocated to the different items purchased in terms of their value on the supplier's invoice. For example, if invoice 1237 (above) had been for 300 Raleigh RC bicycles at $338.75 each, and 200 Raleigh Bombers at $169.38, the total cost of R1 393 690 would have been allocated as follows:

Unit price: Raleigh RC $\frac{\$101\ 630}{\$135\ 507}$ x R1 393 690 ÷ 300 = R3 484 (rounded)

Unit price: Raleigh Bomber $\frac{\$\ 33\ 877}{\$135\ 507}$ x R1 393 690 ÷ 200 = R1 742 (rounded)

6. RECORDING THE COST OF THE GOODS RECEIVED IN THE INVENTORY MASTERFILE

Tania Koetzee (purchases clerk) will enter the cost of the goods received onto the masterfile which is resident on the AS 400 system. This is done as soon as the costing has been carried out so that the masterfile is kept right up to date. Note that the quantity field has already been updated by the GRN. At the end of each day, a dated ***inventory transaction report*** is generated. This report is a list of all inventory items which have had their quantities increased, by how much, and the unit cost price entered. The report is handed to Zodwa Mashego who checks it for accuracy and completeness against the relevant GRNs and costing schedules where applicable. She signs to acknowledge this check. As a double control, Ruth Taylor rechecks the ***inventory transaction report*** to the GRNs the following day.

7. PAYMENT OF CREDITORS – LOCAL SUPPLIERS

7.1 Recording of purchases from local suppliers

As indicted earlier, the acquisitions and payments cycle is not integrated into the other cycles on the AS 400. Tania Koetzee (purchases clerk) is responsible for recording purchases and maintaining a creditors masterfile on her computer using the inhouse developed software. Remember that there are not that many local suppliers. The following documentation is kept in the purchases department in temporary files by sequence number (n) or alphabetically (a).

* Local inventory order reports (n)

* Purchase orders (n)
* Goods received notes (n)
* Invoices as they arrive by fax, email or post from the supplier (a). These invoices will not only be for inventory purchases, but other items purchased on credit as well, e.g. packaging, stationery, invoices from service providers, including shipping agents, etc.
* Supplier delivery notes and statements (a).

About every two days Tania Koetzee enters invoices she has received onto her system. This means that the creditors masterfile is kept up to date. Before entering an invoice, Tania Koetzee

* matches details on the invoice to the relevant purchase order and GRN (which can all be tied together by the purchase order number), or to other supporting documentation in respect of invoices for which no physical goods were received
* checks the prices to the inventory order report and purchase order (or other sources for non-inventory items)
* reperforms extensions, casts and VAT calculations
* checks that the supplier invoices contain the necessary detail so that a valid VAT input credit can be claimed.

If an invoice is incorrect, e.g. ProRide (Pty) Ltd has been charged for goods which have not been received, she confirms the detail against the discrepancy report and supplier delivery note if applicable, and notifies the supplier. The invoice is placed in a pending file to await a corrected invoice from the supplier. This essentially means that the purchase journal and creditors masterfile are updated for the correct amount owed even if it means a delay in recording.

When Tania Koetzee is ready to enter the invoices into the purchase journal (much like an Excel spreadsheet) she accesses the "enter invoices" module (to which access is restricted). To enter the details off the invoice, Tania will key in the supplier's name taken from the invoice. This will bring up a screen which is populated with the supplier's details and formatted to receive only the necessary information to update the creditors masterfile and purchase journal, i.e. the description of the goods purchased unit selling price etc, is not required. Tania therefore enters only the

* supplier invoice number (supplier name is already there)
* the account code to which the invoice must be allocated, e.g. inventory, packaging, maintenance, shipping charges
* the amount of the invoice and the VAT
* the terms of the invoice, e.g. 30 days, 60 days.

On selecting the "enter" option, the purchase journal file and the suppliers account in the creditors masterfile are updated. There are a number of basic programme controls over input, e.g. alphanumerics, missing data (all fields must be completed) and the entire entry process reflects the concept of minimum entry.

During the course of the month, Tania Koetzee will reconcile statements received from creditors with the creditor's account in the creditors masterfile.

7.2 The actual payment of creditors

Up until a few years ago, all local creditors were paid by cheque. This policy has changed and all payments are made by EFT. Payments to creditors are made on the 28th of each month and creditors are paid on the strength of a valid invoice (not on a reconciled creditor's statement) which has been entered on the ProRide (Pty) Ltd system.

* ***Payment preparation***
  This is a "manual" procedure conducted by Zodwa Mashego or Tania Koetzee. Whoever is preparing the schedule on that day will compile a list of suppliers to be paid which includes the amounts that are to be paid, the invoices which are being paid and the name and account number of the supplier. The schedule is prepared on the screen with the information being taken from the creditors masterfile. The schedule is printed out, checked by the other purchases clerk, signed by both clerks and Ruth Taylor (purchasing manager), and given to Johan Els the financial manager, along with the supporting documentation.

None of the terminals in the purchasing section have the bank's software loaded on them and EFT payments cannot be made from them. On receipt of the schedule, Johan Els will carefully check the detail on the schedule to the supporting documentation (initialing it as he does so). He will then access the EFT creditors payment module and enter the detail of the payments to be made. ProRide (Pty) Ltd has a full range of controls over EFT payments as described in a number of chapters in this text and they will not be repeated here. (You can refer to the description of ProRide's payroll system for a description of the detailed controls).

8. PAYMENT OF CREDITORS – FOREIGN SUPPLIERS

There are essentially three parties which must be paid. They are

* the forwarding agent who administers the shipping of the goods.
* the clearing agent who administers the clearing of the imported goods through customs.
* the supplier.

8.1 The forwarding agent and the clearing agent

This is a simple process. As we indicated earlier, ProRide (Pty) Ltd deals with only one company which forwards (ships) and clears its imports. This company makes payments to the various other parties on behalf of ProRide (Pty) Ltd. It then invoices ProRide (Pty) Ltd for the entire amount owed to it. ProRide (Pty) Ltd treats this account like any other local creditor.

8.2 The supplier

The supplier is paid when the conditions of the Letter of Credit have been met. This is essentially when ProRide (Pty) Ltd's bank receives the necessary documentation namely, the Bill of Lading (duly stamped by the customs authority) and the invoice. The bank will not pay unless the documentation is complete and meticulously correct. Once they are satisfied they will transfer the money to the supplier's bank and debit ProRide (Pty) Ltd's bank account.

8.3 Updating the LC Payment Register

When the transfer has taken place it will immediately be revealed on the daily bank statement which is downloaded through the Internet. Ruth Taylor will manually update the LC payment register by debiting the foreign suppliers account. Selma Green (cash book clerk) is also notified of the payment and can update the cash book on her terminal.

9. UPDATING THE GENERAL LEDGER ON THE AS 400 SYSTEM

As we pointed out earlier, the purchases/creditors system is not integrated with the general ledger on the AS 400 system. At month end Johan Els (financial manager) compiles the necessary journal entries for purchases, creditors and cash book transactions and enters them into the general ledger on the AS 400. This entry is checked in detail by the IT manager Gary Powell and the financial director Brandon Nel.

AUDITING THE CYCLE

1. INTRODUCTION

As the name suggests, the acquisitions and payments cycle deals with the goods (and services) which a company purchases, and the payment by the company for those goods.

The acquisitions phase of the cycle is concerned with ensuring that the company acquires only those goods (and services) which it needs and that the goods are of the necessary quality and price. The payments phase of the cycle seeks to ensure that only goods which have been validly ordered and received are paid for and that the payment is authorized, accurate and timeous.

Obviously companies do not only buy goods for resale or manufacture. Depending on the nature of the company's business, there will be expenditures on advertising, travel, consumables, entertainment, stationery or items of plant and equipment. However, whatever the "acquisition" is, the principles of controlling the expenditure remain the same, i.e. only expenditure ***relating to the business*** should be incurred, it should be ***authorized before*** it is incurred, it should be appropriately recorded, and the payment for the acquisition should be the ***correct amount*** and should be ***authorized***. The authority for incurring the expenditure may differ, e.g. for an inventory item it may be a requisition signed by the warehouse manager, and a purchase order signed by the chief buyer. For travel expenses, it may be an authorized budget and a travel approval form signed by a department head, and for the acquisition of an item of equipment, it may be an authorized budget and a directors' minute. Payments are usually authorized by the signature of a department head on supporting documentation after suitable scrutiny. Payments of different amounts may be authorized at different levels.

In most reasonably sized businesses, the vast majority of acquisitions (other than for large items of plant and equipment which is financed in a variety of ways) will be made on "credit" which simply means that the goods or services etc, will be paid for some time after the goods are received, say 30 days or 60 days later, depending on the terms agreed with the supplier. This means that at any point in time the company will have creditors. So in effect, the acquisitions and payments cycle gives rise to ***transactions*** and an ***account balance*** both of which will need to be considered by the auditor in carrying out the audit of the cycle.

The audit of the cycle consists of two parts. In terms of ISA 315 (Revised), the auditor is required to identify and assess the risk of material misstatement at both financial statement level and at account balance and transaction level. This means that in the context of this cycle, the auditor will need to evaluate whether there is anything in the assessment of risk at financial statement level which may filter down into the audit of the cycle and whether there are specific risks pertaining to the creditors balance in the AFS or to the recorded purchase or payment transactions. For example

* at financial statement level : if there is an incentive for the directors to manipulate the financial statements, one of the ways they may do so is by understating the accounts (trade) payable balance

* at account balance level : there may be an identified risk that the creditors balance is understated due to a failure to raise the liability for goods received just prior to year end

* at transaction level : risk assessment procedures may have revealed that purchase orders can be made out and placed by the purchase order clerk without authority, or that employees authorized to make EFT payments share passwords for "convenience sake" and that there is no independent reconciliation of EFT payments after they have been made to source documentation.

Once the cumulative effect of the identified risk has been assessed, the auditor will be in a position to plan "further" audit procedures and "other" audit procedures. Before moving onto the second part of the audit of the cycle, i.e. the response to assessed risk, it is perhaps necessary to remind ourselves of the assertions relating to the transactions in the cycle and the related balance, i.e. accounts payable.

2. ASSERTIONS AND THE ACQUISITION AND PAYMENTS CYCLE

2.1 Purchase transactions

* ***occurrence :*** purchases recorded actually occurred, they are not fictitious and they pertain to the entity
* ***accuracy :*** purchases have been recorded appropriately (i.e. at the correct amount)
* ***cut-off :*** purchases have been recorded in the correct accounting period
* ***classification :*** purchases have been recorded in the proper accounts and
* ***completeness : all*** purchases that should have been recorded have been recorded

2.2 Payment transactions

* ***occurrence*** : payments recorded actually occurred (not fictitious), and pertain to the entity
* ***accuracy :*** the payments have been recorded appropriately (i.e. at the correct amount)
* ***cut-off :*** payments have been recorded in the correct accounting period
* ***classification :*** payments have been recorded in the proper accounts and
* ***completeness : all*** payments (to creditors) that should have been recorded have been recorded

2.3 Trade payables

* ***existence :*** creditors actually ***existed*** at reporting date, (they are not fictitious)
* ***obligation :*** all creditors included in the balance represent ***obligations*** of the company
* ***completeness :*** all creditors that should have been recorded at reporting date have been included
* ***valuation :*** creditors have been reflected at the appropriate amount (at the correct carrying value)

2.4 Presentation and disclosure

In addition to the assertions applicable to the transactions and balance identified above, the directors are also representing (asserting) that the presentation and disclosure of all matters pertaining to the balance and transactions in this cycle are ***complete*** in terms of the chosen accounting framework, have been correctly ***classified*** and ***accurately*** presented and disclosed in an ***understandable*** manner.

3. FRAUD IN THE CYCLE

3.1 Fraudulent Financial Reporting

The most common way of manipulating the financial statements in this cycle is the

* ***understatement of trade creditors(trade payables) :*** this will usually be done to improve the ratios in the working capital sector of the statement of financial position or to avoid a net liability position. Auditors will conduct comprehensive completeness testing on creditors where they believe such a risk exists.

* a common way of understating creditors is to manipulate "cut-off" at year-end, e.g. accounting ***after*** year-end for a purchase of inventory made ***prior*** to year-end, ***but*** including the inventory purchased in the inventory on hand at year-end. This also has the benefit of increasing profits, so all round the financial statements look much better.

* Of course if the directors objective was to reduce profits they could do so by fraudulently increasing purchases.

* Where companies trade with numerous related parties, manipulation of trade payables becomes much easier.

3.2 Misappropriation of Assets

As this is a cycle which actually deals with outflows from the business (i.e. payments), there are real opportunities for management and employees to misappropriate cash and to a lesser extent, goods

* ***ordering of goods by employees or management for their personal use and having the company pay.*** This will amount to the inclusion of invalid purchases (occurrence), and, if the creditor has not been paid by year-end, the inclusion of fictitious creditors (obligation). For this type of fraud to be effective, the perpetrator has to get the goods that have been ordered,

this can be done in numerous ways such as colluding with receiving or warehouse staff, or having the supplier deliver to an address other than that of the company. A similar "misappropriation" which does not involve physical goods and may be easier to perpetrate, would be for a director/manager to have the company pay for personal air flights and have the purchase/payment recorded as business travel.

* ***making completely fictitious payments to creditors*** (occurrence of purchases/obligation of creditors). This is plain theft where those with the power to authorise payments (e.g. cheque signatories, EFT signatories), authorise payments to their own companies, friends, etc. No goods change hands and false documentation is produced.

* ***company claims VAT to which it is not entitled*** (completeness of liabilities). This is very often a "by-product" of the frauds described above.

* ***directors or employees accepting bribes from suppliers as an inducement to purchase goods from that (supplier) company***. This is a difficult situation because from a financial reporting perspective there may be absolutely no problem. The goods purchased may be of the required quality and price, the order properly authorised etc. The payment of the bribe may well be a problem in the supplier's business but is in effect "outside" the business of the company at which the person receiving the bribe is employed. Accepting this type of inducement is likely to be in contravention of the company's employment policies. In terms of Sec 45 of the Auditing Profession Act, where directors receive such inducements, there may be a reportable irregularity. Directors or employees setting themselves, family or friends up as suppliers and then directing business to those entities is a variation of this practice and is effectively, a related party transaction.

* ***theft of goods at the receiving stage*** (existence of inventory). This will normally be an employee fraud, and amounts to receiving clerks signing for goods received but not taking custody of all the goods signed for. The goods which are stolen are sent out on the truck in which they were delivered and off loaded elsewhere. Collusion with the supplier delivery staff is required.

4. FURTHER AUDIT PROCEDURES

4.1 Overall responses to the risk of material misstatement at the financial statement level

In terms of ISA 330, the auditor must implement overall responses to address the assessed risk of material misstatement at the financial statement level. For example

* assigning more experienced staff to the audit, e.g. this could be a response to the risk of manipulation of the financial statements by understatement of the trade payables balance

* emphasizing to the audit team the need to maintain professional scepticism, e.g. to be alert to the possibility that management may be having personal expenditures paid for by the company

* providing more supervision.

4.2 Tests of controls and substantive tests

The auditor's further audit procedures will be a mix of tests of controls and substantive tests. When assessing risk at the assertion level, there is an underlying expectation on the part of the auditor that the controls are operating effectively and essentially that they provide a foundation from which the substantive tests can be developed. Simply expressed, if the controls are very strong, the auditor can place more reliance on the totals and amounts produced by the accounting system and will be able to perform less substantive testing and possibly substantive tests of a different nature. Timing of substantive testing could be also affected.

4.3 The auditor's toolbox

As we discussed in Chapter 5, in terms of ISA 500, the auditor has the following types or categories of audit test available to him

* Inspection
* Observation
* External confirmation
* Recalculation
* Reperformance
* Analytical procedures
* Inquiry

These tests are not specific to a particular phase of the audit and can be used as risk assessment procedures, tests of controls or substantive tests.

4.4 Significant risks

In terms of ISA 315 (Revised), a significant risk is an identified and assessed risk which, in the auditor's judgment, requires special audit consideration. This does not mean that the auditor needs to be familiar with a whole new range of audit procedures (have additional tools in his toolbox), but it does mean he will look closely at the nature, timing and extent of the further audit procedures as well as the skills and experience of the audit team.

In the context of this cycle, significant risks may include

* the risks of fraudulent practices as discussed in point 3 above
* significant acquisitions being made from related parties, e.g. companies within the group or entities owned by a director
* the risk of the understatement of trade and other accounts payable.

5. TESTS OF CONTROLS

5.1 Objective

The auditor tests a control to determine whether the control has been effective in achieving the objective for which it was implemented in the first place. For example, in the context of this cycle, one of the objectives of the control activities implemented by the company, will be to ensure that purchases (acquisitions) of goods are made only for the company. To achieve this objective the controls implemented might be that no goods may be purchased without an official purchase requisition which is signed by the warehouse manager, and an official purchase order which is prepared by a purchase order clerk and approved by the senior buyer. The auditor is interested in this control because if it is effective, he will have gained some evidence that the purchases recorded in the accounting records do not include purchases which were made by employees for their own use (and which were subsequently paid for by the company). To extend the example, the company will want to ensure that all goods ordered were received, and only goods that were ordered and received, are paid for. The controls implemented by the company to achieve these objectives will include, the physical checking of the goods by the receiving clerks, the completion of a GRN and careful scrutiny by reasonably senior personnel before payment is authorized. The auditor's interest in whether these controls are functioning is obvious; if all the controls are working effectively, the auditor obtains worthwhile evidence that the purchases recorded actually occurred, were authorized and were accurately and completely recorded and processed.

5.2 Timing

The auditor needs to gain evidence that the controls on which he intends to place reliance were operating throughout the financial year under audit, so these tests of controls may be carried out at different stages throughout the year during interim visits to the client. However, much of the evidence that a control has worked throughout the year, may be revealed by the audit trail which is created. For example, the auditor could choose a sample of recorded purchases from throughout the year and test that the supporting purchase documentation consists inter alia, of a signed purchase requisition and approved purchase order. This doesn't prove that the purchase requisition and purchase order were authorized ***before*** the order was placed, but combined with other evidence which the auditor will seek, e.g. about the receipt of the goods and the payment for the goods, strong persuasive evidence that the controls were functioning ***at that time*** will have been gathered. If however, the auditor discovers that there are GRNs and supplier invoices which are ***not*** supported by an approved requisition and purchase order, he gains evidence that the controls were (are) not effective. This is likely to increase the substantive tests which will need to be carried out.

5.3 The nature of tests of controls

As pointed out earlier in this section, the auditor uses an assortment of procedures when conducting tests of controls in this cycle. Controls in this cycle will vary from company to company and the auditor will need to select a suitable mix of procedures to achieve his overall objective of determining whether the controls implemented were (are) effective. This can be illustrated as follows

Inspection

* a sample of recorded purchases could be selected and the supporting requisition and purchase order could be inspected for an authorizing signature
* a sample of purchase orders could be compared to the list of approved suppliers to confirm that purchases are made only from approved suppliers. This procedure may be supplemented by ***inquiry*** and inspection of supporting documentation which provides evidence that a supplier is only added to the list of approved suppliers after a thorough and independent evaluation of the supplier. This reduces the risk that purchases can be made from businesses connected to the company's order clerk, buyer or members of management, and that purchase of goods which are not for the company's use, can be made.
* inspect the masterfile amendment log and supporting documentation for indication of approval for the addition of a supplier to the creditors masterfile during the year.

Note : in some systems there may be no visible indication of approval of say, the purchase order as it is given "on the system". This on-screen approval might be effected by the purchase order clerk being unable to print out or email a purchase order until approval has been given by the employee (chief buyer) whose access profile permits approval of purchase orders. The appropriate test may be for the computer audit division to look at and test user profiles as part of a system orientated CAAT. Alternatively, the auditor may be able to infer (assume) that approval of the purchase order does in fact take place if other tests of controls in the process, e.g. controls over payments to creditors, prove to be effective.

Inquiry

* e.g. inquire of the receiving clerk as to
  - the procedures he follows when goods are delivered
  - what happens to goods that are delivered but are not as listed on the purchase order (wrong goods, short delivered, over delivered)
* inquire of the purchase order clerk as to what procedure is followed for placing an order if there is no purchase requisition provided, e.g. he gets a verbal instruction to place an order
* inquire of the financial accountant (or similar) as to what happens when a payment by EFT must be made and one of the individuals required to "authorize" a payment, is not available

Note : questions put to employees should be expressed in a way which requires more than a "yes" or "no" response. In this way the auditor will learn more about the effectiveness of the control and may be provided with information he least expected.

Observation

* observe the procedures which are carried out by the receiving clerk when a delivery is received from a supplier
* observe the "authorize" and "release" procedures being undertaken for the payment of a creditor.

Note : observation is not a very convincing procedure as the employee is likely to do what he is supposed to do because he knows the auditor is watching! Observation would always be matched with other procedures, for example when observing the receiving of goods, the auditor may request the receiving clerk to insert an invalid purchase order number into the system to see what happens (it should be rejected).

Reperformance

The auditor may choose to reperform a sample of creditors' reconciliations.

With regard to accuracy and completeness of processing and recording of transactions promptly and in the correct accounts, especially in integrated real-time systems, current accounting software is very fast, efficient and reliable. The auditor is likely to concentrate tests of controls on controls over the authorization of transactions and the controls over reviewing and reconciling the results of processing, e.g. logs, reports, listings, etc. If these controls appear to be operating successfully, the auditor can assume that processing controls are effective.

6. SUBSTANTIVE PROCEDURES

6.1 Nature

In auditing the cycle so far, the auditor has carried out procedures to

* identify and assess the risk of material misstatement and
* gather audit evidence about the operating effectiveness of the controls (tests of controls).

The auditor is now required to conduct substantive tests which as we have seen, are designed to detect material misstatement at the assertion level. Substantive tests consist of

* tests of details of classes of transactions, account balances and disclosures, and
* substantive analytical procedures

The difference between tests of detail and analytical procedures is that the former consists of auditing the detail of the transaction, account balance or disclosure whilst the latter provides more general or overall evidence. The types of procedure carried out will still be those listed in point 4.3 with the obvious exception of analytical procedures. For example, in carrying out a test of detail on a purchase invoice, the auditor would ***inspect*** the supporting documentation and agree dates, cross-referencing, amounts etc, and may reperform the casts, extensions and VAT calculations. When conducting substantive analytical procedures, the auditor does not consider the detail but rather the "overall picture". He will compare totals of transactions and account balances to the same totals and account balances for different periods, or consider changes in the make up of totals in relation to other periods or industry norms etc, with the intention of identifying any strange or unusual fluctuations. For example, the auditor may compare balances on individual creditor's balances year-on-year and follow up on any major or unexpected differences, or he may calculate ratios such as total purchases divided by accounts payable, again for comparison to prior years.

In terms of ISA 330, the auditor must design and perform some substantive procedures for each material class of transaction, account balance and disclosure, regardless of the assessed risk of material misstatement. In other words, the auditor cannot decide that because he has assessed the risk of material misstatement as low, and because his tests of controls provide persuasive evidence that controls had operated effectively for the period under review, there is no need to do any substantive testing. The reason behind this is that

* risk assessment is judgmental and the auditor may not have identified all risks, and
* internal control has inherent limitations, including management override, e.g. an employee who refused to authorize a purchase order because it was not for goods used by the company, may have been overridden by a senior member of management wishing to have the company purchase the goods for his own personal use.

However, the auditor does not necessarily have to carry out both tests of detail and analytical procedures. If assessed risk is judged as low and tests of controls indicate that controls are operating effectively, the auditor may decide that all that is required to reduce audit risk to an acceptable level, is the performance of ***analytical*** procedures. In practice it is common for the auditor to use a combination of tests of detail and analytical procedures when conducting substantive tests.

6.2 Timing

Most substantive testing takes place at or after year-end. This is logical as these tests are aimed primarily at gathering evidence about the account balances and disclosures in the financial statements. In practice however there is often an audit deadline (a date by which the audit must be completed) which forces the auditor to carry out extensive substantive (and other) testing at an interim date, say two months prior to year-end. In the context of this cycle, the auditor may choose to conduct substantive procedures to verify the balance on the trade payables account at the 10 month period and then "update" this work for the year-end trade payables account by conducting tests on the remaining two months, during the two months and at year-end. These tests which will be a mix of tests of controls and substantive tests, are termed "roll forward tests".

6.3 Extent of testing

The extent of substantive testing is generally regarded as being a function of (determined by) the assessed risk of material misstatement and the results of tests of controls. In general, the greater the risk of material misstatement, and the less effective the controls appear to be, the greater the amount of substantive testing. In the case of substantive testing of disclosure, qualitative materiality will be an

important factor. For example, the substantive testing of the disclosures relating to director's emoluments is likely to be both detailed and extensive. The extent of testing is usually reflected in the size of samples used for testing as well as the type of tests being carried out.

Overall the auditor is required to obtain sufficient appropriate evidence to satisfy himself that audit risk has been reduced to an acceptable level.

7. SUBSTANTIVE TESTING OF TRANSACTIONS IN THIS CYCLE (by assertion)

7.1 Purchases

The following example illustrates the substantive audit procedures (by assertion) which the auditor may conduct on a purchase transaction. Assume that a purchase has been selected from the purchase journal of a manufacturing company, ExWhy (Pty) Ltd.

* ***Occurrence*** (the recorded transaction has occurred and it pertains to ExWhy (Pty) Ltd).

- inspect the supporting documentation (purchase order, supplier delivery note, GRN and invoice) to confirm
  - that the (external) documents are made out to ExWhy (Pty) Ltd and are from an approved supplier
  - all documents are correctly cross-referenced to each other
  - each document is signed by the designated authority e.g. chief buyer, receiving clerk
  - the goods purchased are of a type used by the company
- inspect the cash payments records/EFT schedules/bank statements to confirm that the goods were appropriately paid for; payment authorised, correct payee, correct amount (see Note (a)).

* ***Accuracy*** (the amount of the purchase has been recorded appropriately)

- confirm the mathematical accuracy of the invoice by recalculating all extentions (quantity x price), casts and discounts
- agree the quantity of items charged on the invoice, against the quantity on the goods received note
- confirm prices and trade discounts used on the invoice by inspection of the order or purchase contract
- recalculate VAT, and by inspection of the invoice, confirm that discounts are taken into account prior to the calculation of VAT
- by inspection, confirm that the VAT number and details of the supplier as well as the supplier's VAT number are clearly presented on the supplier tax invoice. (For a valid input credit to be recorded, a valid supplier tax invoice is required).

* ***Cut-off*** (the purchase has been recorded in the correct accounting period)

- inspect the dates on the supplier delivery note, goods received note and invoice to confirm that the goods were received during the accounting period under audit. (The date on these documents should also coincide with the month in which the purchase is recorded in the purchase journal).

* ***Classification*** (the purchase has been recorded in the proper accounts)

- inspect the purchase order to determine the expense or asset account to which the purchase should be allocated and posted (this should have been entered on the purchase order by the buyer) and trace the posting from the purchase journal to the designated expense or asset account in the general ledger
- establish the description of the goods purchased (by inspection of the purchase documentation) to confirm that the classification of the purchase is appropriate e.g. the purchase of a non-current asset has not been written-off as an expense
- inspect the purchase journal (and invoice) to confirm that VAT has been correctly allocated and posted
- inspect the supplier's account in the creditors ledger to confirm that the purchase was correctly posted from the purchase journal.

* ***Completeness*** (all purchases that should have been recorded have been recorded).

- to test the completeness of purchases, the auditor will test from a document recording the receipt of the item purchased to the recording of the purchase in the records. The auditor may choose a random sample of GRNs from the sequence of GRNs and trace them through to the corresponding invoices. Tests of detail would then be carried out as described above. If there was no corresponding invoice, the purchase may not have been recorded.

Note (a) Strong corroborative evidence for the occurrence assertion is obtained if a properly authorized payment for the purchase is recorded. The auditor is likely therefore, to extend the testing of his sample of purchases to include the testing of the corresponding payment.

Note (b) Some of the procedures described above may be regarded as "tests of controls", e.g. inspecting the purchase order to confirm that it was made out to an approved supplier, or checking for authorizing signatures. This is not an issue as the auditor frequently carries out "dual purpose tests" which provide some evidence of the effectiveness of controls and some substantive evidence. In the context of the audit, this may be an efficient way of gathering evidence.

Note (c) For some of the purchases made by the company, there may be no specific purchase order or goods received note to tie to the invoice, e.g. the purchase of a service or a non-physical item which is not "delivered", such as travel expenses or delivery charges. In these instances, the auditor will still test the accuracy of the invoice but will seek alternative source documentation to support the purchase.

7.2 Payments

Tests of detail on payments will again concentrate on the assertions relating to transactions. As indicated earlier, a payment in the context of this cycle is normally linked directly to a purchase and the auditor may extend his tests of detail on purchases to the corresponding payment. However, the auditor also wants evidence that payments recorded in the cash book were in respect of ***actual*** valid purchases which occurred. The auditor may therefore select a sample of payments from the cash payments journal and test as follows

* ***Occurrence***

- obtain the invoice supporting the payment
- inspect the invoice to confirm that
  - it is made out to ExWhy (Pty) Ltd
  - is for goods, services or other expenditures normally used or incurred by the company and is from a supplier on the approved supplier list
- inspect the authority for the payment, e.g.
  - appropriately approved purchase order, GRN
  - appropriately approved expenditure requisition or claim, e.g. travel expenses authorization
  - approved payment requisition

* ***Accuracy*** (the amount of the payment has been recorded appropriately)

- reperform the casts and calculations on the invoice
- agree the amount of the invoice to the payment in the cash payments journal.

* ***Cut-off*** (the payment has been recorded in the proper accounting period)

- inspect the dates on the payment, the invoice and supporting documentation to confirm they fall within the period under audit and are reasonable in relation to each other.

* ***Classification*** (the payment has been recorded in the proper accounts)

- trace the payment to the general ledger and creditors ledger to confirm that the posting has been made to the creditors control account and the correct creditor in the creditors ledger
- where "the purchase" has not gone through the purchase journal (not raised as a creditor), confirm by inspection of the description on the invoice or payment requisition, that the payment has been allocated and posted to the correct account in the general ledger, e.g. travel expenses.

* ***Completeness*** (all payments that should have been recorded, have been recorded).

The situation where a payment has been made but has not been entered in the cash payments journal should be revealed by inspection or reperformance of the bank reconciliation statement.

Note (a) The auditor may also wish to perform tests of detail on a sample of payments reflected in the individual creditors accounts. Similar tests to those described above would be carried out.

Note (b) Where the payment has been made by cheque, the auditor would inspect the returned cheque to confirm that it was signed by authorized signatories and that it was made out to the correct payee. Where payment was by EFT, the auditor will inspect the applicable schedule of EFT payments for authorizing signatures and will inspect the audit trail/bank statement/remittance advice, to confirm that the EFT was made to the correct payee. The auditor will also consider the extent to which he can rely on those senior officials who have the "authorize" and "release" privileges for EFTs to carefully check the payment details before the EFT is made.

7.3 Substantive analytical review procedures

* The auditor will supplement his tests of detail by conducting some analytical procedures. These may include
  - comparisons of expenditure categories month to month or to prior periods, e.g. purchases of goods for resale, travel costs, advertising, repairs and maintenance, consumables, motor vehicle expenses, etc.
  - calculation of each expense as a percentage of say, gross profit or total expenses and comparison of the percentages to prior periods
  - comparison of actual expenses to budgeted expenses.

* Abnormal fluctuations would be followed up by
  - vouching material fluctuations by tracing entries to source documentation for investigation, e.g. valid expense, correct amount recorded
  - discussion with management.

8. SUBSTANTIVE PROCEDURES ON THE TRADE AND OTHER PAYABLES BALANCE

The main thrust of substantive testing in this cycle will be on the trade and other payables account balance at year end. Current liabilities on the statement of financial position will often be made up of other balances which may include short-term borrowings, bank overdrafts, taxation payable etc. The most material balance is usually trade and other payables (often referred to as trade creditors) and the audit procedures which follow relate primarily to the audit of trade and other payables. In practice, trade and other payables are often referred to as trade creditors, accounts payable etc, all of which are generally intended to mean creditors arising out of trading activities. To an extent, we have used the terms inter-changeably.

8.1 Assertion : obligation - the trade payables represent obligations pertaining to the company

The evidence for the obligation assertion is supplied by inspecting the supporting documentation, statements, invoices, etc to confirm that they are:

* made out in the name of the company
* in respect of purchase of goods (or services) which are used by the company.

This inspection will take place when creditors' reconciliations are audited as a year-end valuation procedure and when any tests of transactions are conducted.

8.2 Assertion : existence - trade payables included in the balance actually exist, they are not fictitious

The existence assertion for trade payables is usually a low risk assertion as companies do not normally wish to overstate their liabilities, so in the absence of any contrary evidence, the auditor can assume that the trade payables (and other liabilities) which appear in the statement of financial position, do actually "exist" . The auditor will however, perform "cut off" tests at year-end, to confirm that purchases and creditors have not been overstated and have not been prematurely raised. Bearing in mind that if management are intent on overstating purchases/creditors to manipulate the financial statements, they would do it for material amounts, the auditor should:

* record the number of the last GRN for the year (cut-off number)
* select from the purchase journal, ***material*** purchases entered during the last two weeks of the year and trace to the relevant GRN and supplier delivery note (via the invoice)
* inspect these documents to confirm that the GRN number is lower than the cut-off number and that the documents are dated prior to the year end date.

  These tests should reveal whether the company is holding the purchases journal "open" into the next financial year in an attempt to manipulate the figures at financial year end. (Note: the intention of these tests is to determine whether the liability existed at year-end).

8.3 Assertion : valuation - trade payables are included in the financial statements at appropriate amounts

The carrying value of trade payables will in effect be the total amount of trade payables (and accruals) because unlike asset accounts, there is no need to write-down the balance (make allowances) for obsolescence, depreciation, impairments or bad debts :

* agree the list of individual creditor's balances to the balance on the creditors control account
* agree a sample of individual creditor's balances on the list to the individual creditor's account in the creditors ledger
* agree the total of the accrual and creditors control accounts in the general ledger to the trial balance
* reperform casts of the creditors control account, and the creditors list
* identify any debit balances on the creditors list, establish the reason with the purchases manager and consider whether the balances should be transferred to debtors
* select a sample of creditors (which includes the company's major suppliers) from the creditors list and obtain the year-end creditors reconciliations performed by the creditors clerks
  - reperform the casts of the reconciliation
  - agree balances on the reconciliation to the creditors statement and creditors listing
  - test the logic of the reconciliation
  - by inspection of the supporting documentation and by inquiry and confirmation, confirm the validity of reconciling items
* if applicable, select a sample of foreign creditors from the creditors list and by scrutiny of the supporting documentation (invoice), determine the amount owed to the creditor in the foreign denominated currency
* obtain from a financial institution or suitable publication, the applicable currency exchange rate at the financial year end (spot rate) and
  - using the spot rate, compute the amount owed to the creditor at the financial year-end in local currency (rands)
  - compare this amount to the amount recorded for the creditor on the creditors list and, if necessary, request adjustment. The foreign creditor will have been raised initially at the rate ruling at transaction date i.e. the date on which the risks and rewards of ownership passed, and may require adjustment for any change to the exchange rate

  Note: the creditors balance will be written up or down, and the corresponding entry will be to an exchange loss or gain.
* obtain a list of accruals from the client
  - cast the list
  - agree the total on the list to the account in the general ledger, the trial balance and the statement of financial position (the amount will be included in creditors)
* agree amounts recorded on the accrued list to invoices, statements, etc, and reperform any calculations, e.g. leave pay accrual.

8.4 Assertion : completeness - all trade payables and accruals which should have been recorded have been recorded

It is generally considered that completeness is the assertion most at risk of material misstatement as the company is more likely to understate its liabilities than overstate them. The auditor is therefore concerned about what is ***not*** in the account but should be, so completeness tests are focused on identifying unrecorded liabilities

* compare the list of creditors at the current year-end to the previous year-end, to identify:
  - creditors on the previous list who do not appear on the current list, and
  - creditors balances which are significantly smaller at the current year-end

- and by enquiry and inspection, determine and evaluate the reason

* inspect the creditor's correspondence file for correspondence relating to unsettled disputes with suppliers, and by discussion with management, determine whether any adjustments to creditors are required, e.g. the audit client may be disputing the actual delivery or condition of the goods delivered and may not have raised the liability
* if available, inspect the list of GRNs which were unmatched to invoices at year-end. (This list should have been obtained by the auditor at year-end when document cut-off numbers were taken). Confirm by inspection, that a journal entry raising the corresponding creditors at year-end, has been passed, and that the amounts raised are correctly computed by :
  - obtaining the price of the goods received (from the order or pricelist or corresponding invoice if it has arrived)
  - recomputing the amount owed
* select a sample of material purchases from the purchase journal for the month following the year-end and trace to the goods received note applicable to the purchase, to confirm that:
  - the GRN number is greater than the GRN "cutoff" number (see 8.2)
  - the dates on the GRN and supplier delivery note are ***after*** the financial year-end
* select a sample of large payments from the cash payments journal for the month(s) after the financial year-end and, by inspection of the GRN and delivery note, confirm that if the payment relates to goods or services received ***prior*** to year-end, the corresponding creditor had been raised at year-end
* inspect the workpapers relating to creditors reconciliations to identify any instances of reconciling items which result in understatement of the creditors balance e.g. a disputed amount prematurely written-off, and follow up with management.
* inspect the workpapers from attendance at the inventory count and investigate any instances of physical inventory materially exceeding recorded inventory. This may indicate deliveries received prior to year-end which have been included in physical inventory but for which no entries in the records have been made, i.e. no goods received note or invoice from which to raise the liability
* inspect the general ledger accounts for periodic expenses to determine whether all amounts have been correctly accrued e.g. rent, electricity, have 12 debits to the expense accounts
* perform analytical procedures and follow up on any material fluctuations, e.g.
  - current year purchases, creditors and accruals at year-end to prior years
  - trade payables as a percentage of current liabilities
  - trade payables days outstanding compared to prior years
* enquire of the financial accountant whether suppliers of services (as opposed to goods) who provided the service prior to year-end, have been raised as creditors
* inspect the creditors control account for unusual debit entries
* if necessary, obtain confirmation of balances direct from a sample of creditors i.e. conduct a positive creditors confirmation. It may be appropriate to obtain direct confirmations of:
  - nil balances
  - major creditors (to confirm that the balance is not understated despite being large)
  - balances which have significantly reduced since the prior year
  - creditors for which there are no statements
* include reference to the completeness assertion for trade payables and accruals in the management representation letter.

8.5 Assertions pertaining to presentation and disclosure of trade and other payables

These are not very extensive for trade and other payables

* the auditor must inspect the disclosures and consider whether
  - they are complete in terms of the applicable reporting framework, e.g. the balance is included in current liabilities (as part of accounts payable)
  - the disclosures are consistent with evidence gathered on the audit
  - amounts, facts, details etc are accurate and agreed with the evidence gathered
  - any classification of the information disclosed is appropriate
  - the wording of the disclosures is clear and understandable.

9. "OTHER" AUDIT PROCEDURES

In addition to carrying out risk assessment procedures and further audit procedures, the auditor is also required to carry out "other" audit procedures. These are procedures which are carried out to ensure that the engagement complies with the ISAs. In the context of the audit of any cycle, one of the other procedures to be carried out would be to comply with ISA 265- Communicating Deficiencies in Internal Control to those charged with governance and management. For a summary of this statement you should refer to chapter 10.

10. THE USE OF AUDIT SOFTWARE (SUBSTANTIVE PROCEDURES)

If the company's system is computerised and suitable software is available, it can be very useful to the auditor. The use of audit software to audit the creditors masterfile, is perhaps a little less effective than when using software to substantively test asset accounts. This is because with asset accounts, the auditor is concerned with what is included in the account, whilst with the creditors balance, the auditor is more concerned with what is ***not*** in the records. However, the software can still be put to good use.

10.1 The creditors masterfile can be cast (added) to obtain the total amount owing and a detailed list of creditors and their balances can be printed out. The aging of creditors can also be cast and crosscast to the total.

10.2 The masterfile can be scanned for "error" conditions

* blank fields, e.g. missing account numbers
* debit balances.

10.3 The masterfile for the current year-end can be compared to the prior year masterfile to identify

* significantly reduced balances
* creditors who no longer appear.

10.4 The software can be used to extract samples, e.g.

* amounts above a certain amount
* nil balances.

10.5 The software can be used to extract lists of any creditors which can be identified by a particular field or code, e.g. a creditor with whom the company is in dispute may be identified by the addition of a code to its record.

Note. The creditors masterfile will usually contain the following fields

* account number
* name
* address and contact details
* total amount payable
* aging of total amount payable
* payment and discount terms.

CHAPTER 12

INVENTORY AND PRODUCTION CYCLE

CONTENTS

		Page
ACCOUNTING SYSTEM AND CONTROL ACTIVITIES		12/2
1.	Introduction	12/2
2.	Characteristics of the cycle	12/2
3.	Objectives of this section of the chapter	12/3
4.	Basic requirements for any inventory and production cycle	12/3
5.	Documents used in the cycle	12/4
6.	Warehousing : Function, documents, risks and control activities	12/6
7.	Production : Function, documents, risks and control activities	12/8
8.	Inventory counts : cycle counts and year-end counts	12/11
9.	Computerisation in the inventory and production cycle	12/13
INVENTORY CONTROL AT PRORIDE (PTY) LTD		12/14
AUDITING THE CYCLE		12/18
1.	Introduction	12/18
2.	Financial statement assertions and the inventory and production cycle	12/18
3.	Important accounting aspects	12/18
4.	Fraud in the cycle	12/20
5.	Tests of controls and substantive procedures	12/22
6.	Post inventory count procedures	12/24
7.	The use of audit software	12/27

ACCOUNTING SYSTEM AND CONTROL ACTIVITIES

1. INTRODUCTION

In practice, this cycle is given a number of different names such as the conversion cycle, the inventory and warehousing cycle, etc., so it is important to understand what happens in the cycle. The cycle deals with:

1.1 The custody and safekeeping of inventory in whatever form it is, i.e. goods held for resale or manufacture, and finished goods.

1.2 The recording of costs where a production/manufacturing process occurs.

Because of the diversity of business activities, each organization will have its own specific requirements in relation to this cycle. For example a wholesaler of consumer goods will be concerned only about sound procedures over receiving inventory, keeping it safe and secure for the time that it is in the warehouse, and issuing the inventory to the retailer. The physical form of the inventory is not altered; it comes in, is stored and it goes out when it is sold. A motor manufacturer on the other hand, has a far more complicated cycle to cope with. Component parts must be received and stored, they must then be issued to the production department for the manufacture of the motor vehicle. Once this has occurred, the motor vehicle must be transferred to a finished goods storage area, from where it will be removed (issued) when sold. When a company manufactures an item, it will be necessary to accumulate the costs applicable to producing that item. These consist of the costs of materials, wages incurred in manufacturing the items and production overheads. Part of this cycle's function is to control these costs. Broadly stated, production can take place on a "process cost" basis or a "job cost" costing basis.

* Process costing takes place when a large quantity of like items are manufactured on a production line, e.g. hundreds of plastic chairs are being manufactured day after day.
* Job costing takes place when a unique item (an item with its own specifications) or a small number of the same item are manufactured as a job.

You will also come across combinations of the above, but the principles of controlling costs remain the same.

2. CHARACTERISTICS OF THE CYCLE

2.1 Heart of the business

For most businesses, inventory is the most important part of the organization. The entire organization is often shaped around the type of inventory in which the business deals, i.e. its plant and equipment will be specific to its production; the warehouse will be designed to store its inventory safely and securely and all the other cycles are dependent upon it. Obviously it must be a product that has a market.

2.2 Effect on the financial statements

Inventory is usually the major component in the calculation of cost of sales, gross profit and net profit. It plays a prominent role in the fair presentation of the financial statements and for this reason material misstatement in inventory, in whatever form it comes, will often be pervasive to the financial statements. For this reason and 2.1 above, the accounting system and related control activities within the cycle must be well designed and strictly adhered to, e.g. a strong control environment must be maintained and physical access controls must be in place. Many businesses have collapsed because they failed to control their inventory.

2.3 An internal cycle

This cycle has no direct interface with entities outside the company. The acquisitions cycle "puts in" the inventory and the revenue cycle "takes out" the inventory. Therefore control in the inventory cycle requires good control within these two other supporting cycles. For example, if goods are not properly counted when they are received (part of the acquisitions and payments cycle), the warehouse will not be able to maintain accurate records.

2.4 A physical asset

Because the cycle deals with physical assets (as opposed to "non-physical" book assets e.g. debtors), extensive physical controls are usually required. The reasons for this are obvious

* inventory can be stolen for resale or use, a particular problem when the company deals in consumable items, e.g. clothing, foodstuffs, electronic goods
* physical assets can be damaged, e.g. glass products can be broken, paper products destroyed by fire or water.

Many companies need to go to considerable lengths to protect their inventory and the list of physical controls is endless. Guards, electronic alarms, surveillance, armoured glass (jewellery stores), restricted access, air-conditioning, fire alarms and extinguishing systems, are common methods. Eventually the cost/benefit requirement for internal control comes into play, and companies have to decide on the most effective manner of physically protecting their inventory whilst remaining within their budget.

2.5 Inventory fraud

Because inventory is so central to the fair presentation of the financial statements, directors of companies who wish to manipulate the profits and assets they are reporting, can do so very effectively by manipulating the inventory balance at the year end.

2.6 Diversity of inventory

The accounting system and related control activities must be able to deal with inventory which is diverse in nature, location, permanence and stage of development

*	nature	:	easy to identify, e.g. fridge, cricket bat, vehicle
		:	hard to identify, e.g. chemicals, precious stones
		:	growing or moving, e.g. plants, chickens, game
*	location	:	multiple warehouses
		:	obscure locations
		:	in the possession of others e.g. customs, on consignment
		:	in transit
*	permanence	:	fresh produce
		:	products with expiry dates, e.g. medicine
		:	technological obsolescence
*	stage of development		
		:	raw materials
		:	work in progress
		:	finished goods

This diversity also has an affect on the auditor as the assertions relating to inventory are directly affected by its characteristics, e.g. how does the auditor gather evidence about the ***existence*** of gas, the net realisable value ***(valuation)*** of products which are subject to rapid technological obsolescence, the ***rights*** to inventory held in someone else's possession or the ***completeness and existence*** of inventory held at multiple and obscure locations?

3. OBJECTIVES OF THIS SECTION OF THE CHAPTER

The objective of this section of the chapter is to provide you with a basic understanding of how the cycle fits into the company's activities and why it is so important. We have also provided a broad description of control activities when the cycle also includes a production element.

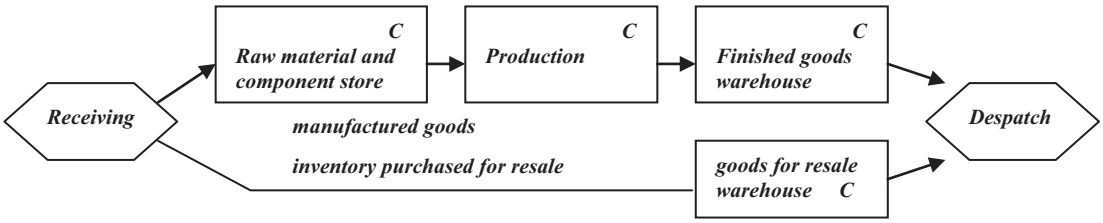
4. BASIC REQUIREMENTS FOR ANY INVENTORY AND PRODUCTION CYCLE

As indicated earlier, the inventory and production cycle is an internal cycle which must achieve three things; it must:

* control the physical transfer (movement) of inventory (in its various forms)
* protect the inventory from damage, loss and theft, regardless of whether it is manufactured inventory or inventory purchased for resale

* plan, control and record the costs of manufacture.

The diagram below represents the cycle in a simple format. It illustrates that goods received from suppliers follow one of two paths, namely, to the raw material and component store, on to production and into the finished goods warehouse, or direct to the "goods for resale" warehouse. The diagram also indicates where a transfer takes place (arrow head) and where physical controls over inventory are required (***C***).



5. *DOCUMENTS USED IN THE CYCLE*

5.1 Goods received note

On transfer of inventory items (of whatever kind) from the goods receiving bay into the warehouse, the warehouse clerk will sign the goods received note which was made out when the goods were delivered by the supplier.

5.2 Materials (components) requisition, materials (components) issue note

A materials (component) requisition is a documented request to the warehouse to release materials or components to the production section, and a materials (components) issue note records the issue of materials to production.

5.3 Manufacturing or production schedules

These documents are used to notify the production/manufacturing department as to what is to be produced. What is to be produced will be decided by an analysis of future sales (forecasts), current inventory holdings of finished goods and specific orders or contracts which have been obtained. The analysis will be committed to a production plan.

5.4 Job cards

A job card is a document which tracks the stages of production for a specific job. As costs are accumulated, e.g. raw materials used, labour hours expended, they are recorded on the job card. At a later stage, an overhead allocation can be made to arrive at the total cost of production.

5.5 Production report

Production reports are documents which are used to report results of production, output, wastage loss, etc. at identifiable stages or completion of production or for specific cost centres.

5.6 Costing schedule

A costing schedule is used to identify and quantify all the costs which it is anticipated will be incurred in manufacturing the company's products. It is in effect a "budget" against which actual production costs can be measured.

5.7 Transfer to finished goods note

This document records the transfer of manufactured goods from the production department into the finished goods stores.

5.8 Picking slip and delivery notes

You will recall from the revenue cycle, that these documents are used to select goods ordered from the warehouse and to assist in controlling the movement of goods once they have been sold.

5.9 Inventory sheet

A document which is used during an inventory count. The inventory sheet will usually contain a description of each item of inventory, its location in the warehouse, and a column into which the quantity of items actually counted, can be entered. The document will usually also contain a column for entering the cost of the item and a column into which the extension of quantity x price can be entered, e.g. 8 items x R40 cost = R320.00.

5.10 Inventory tag

An inventory tag is a small, numerically sequenced cardboard (or similar) tag, which is attached to the different types of inventory before an inventory count. It will be in two distinct, but identical parts which will each contain a tag sequence number, the inventory number and description, and an empty block into which the quantity of inventory on hand will be entered as the inventory item is counted. When the first counting team has counted the number of items for that particular inventory item, they will enter the number in the quantity block of one part of the inventory tag. They will then remove that part of the tag and hand it to the count controller. The second count team will perform a second count and follow the same procedure. The count controller will match the two parts of the inventory tag and any discrepancies will be recounted. This results in an accurate inventory count.

There are a number of variations of the tag system e.g. some tag systems also contain a part which contains the tag number, inventory number and description and remains with the inventory item for identification purposes until the count is completed and all problems have been resolved. (The basic principle remains the same.)

5.11 Inventory adjustment form

The inventory adjustment form is a sequenced document which is used to record adjustments which must be made to correct the perpetual inventory records when actual inventory and theoretical inventory (per the perpetual inventory records) do not agree, e.g. a inventory item which has been stolen will result in the actual "quantity on hand" being less than the "quantity on hand" recorded in the perpetual inventory records. When this is discovered (by counting the inventory) the perpetual inventory records must be corrected.

6. *WAREHOUSING : FUNCTION, DOCUMENTS, RISKS AND CONTROL ACTIVITIES*

WAREHOUSING : GOODS FOR RESALE, COMPONENTS FOR MANUFACTURE AND FINISHED GOODS		
Function	***Documents/records***	***Risks***
The purpose of this function is to 1. Control the transfer of goods in and out of all warehousing facilities, e.g. goods received from "receiving" to the warehouse for storage or finished goods received from production into the finished goods store. 2. Physically protect inventory in all warehouses. "Inventory" in production will also need protection but this is likely to be the responsibility of production personnel.	* Goods received notes * Material (components) requisitions * Picking slip * Material (components) issue note * Delivery note * Transfer to finished goods note * Perpetual inventory records * Inventory count documentation	* Goods received from suppliers are not transferred into the warehouse timeously or at all (stolen) * Inventory (in whatever form) is stolen or lost * Inventory deteriorates in value due to • inadequate physical controls, e.g. gets wet • its nature, e.g. foodstuffs, chemicals * No record is created of goods or components physically moved * The goods or components issued are incorrect resulting in lost sales or production delays * Inventory shortages (including theft) are concealed.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
Controlling the movement of goods, components and finished goods. 1. No movement of inventory should take place without an authorising document, e.g. picking slip, material requisition. 2. No movement of inventory should take place without the movement being recorded e.g. a delivery note and material issue note. 3. Whenever there is a transfer of inventory between sections, e.g. receiving section to warehouse, production to finished goods, both the deliverer and the receiver should acknowledge the transfer by, for example, signing the transfer document after having checked the description, quality and quantity of the items being transferred against the source documents. For example warehouse personnel and production clerks to sign the material issue note after checking the quality, quantity and description of goods being transferred (isolation of responsibilities). 4. Documents should be sequenced and filed numerically. 5. Documents must be sequenced checked and missing documents investigated, e.g. a missing GRN in the warehouse will probably indicate that the goods have not been transferred to the warehouse.

Controlling damage, theft and loss of inventory in all forms, i.e. in warehouses and during production.

1. ***Physical controls*** (the nature and value of the company's inventory will determine the physical controls which are put in place)
   - entry and exit : minimum entry and exit points
   - controlled entry and exit : swipe cards, keypads, turnstiles, gate control, biometric readers, security guards, X ray (e.g. jewellery manufacturer)
   - restricted entry : e.g. buying clerks not permitted to enter warehouse, unaccompanied, only production employees allowed in production facility
   - secure buildings : minimum number of windows, solid structure
   - environmental : areas to be dry, clean, neatly packed, pest free and temperature controlled where necessary
   - surveillance : cameras/video recording over production (e.g. where items are easily stolen off the production line), receiving and despatch areas.

2. ***Comparison and reconciliation***
   - physical inventory (in all its forms) is compared to theoretical inventory per the perpetual inventory (see point 8 for a discussion of cycle counts and inventory counts).
   - actual production is compared to the manufacturing or production schedules
   - actual production is compared to budgets
   - all material variances should be investigated.

7. PRODUCTION : FUNCTION, DOCUMENTS, RISKS AND CONTROL ACTIVITIES

PRODUCTION : PLANNING, CONTROLLING AND RECORDING COSTS		
Function	***Documents/records***	***Risks***
The purpose of production is to manufacture the company's products. Production is essentially a physical activity but in the context of the inventory and production cycle, the production department will be required to 1. Requisition and receive components from the warehouse. 2. Control costs during manufacture. 3. Record actual costs. 4. Account for the items produced and transfer the items to a warehousing facility. 5. Compare actual and budgeted costs.	* Materials requisitions * Materials issue notes * Job cards * Production schedules * Production reports * Transfer to finished goods notes	* Unauthorised requisitioning or issue of materials (theft) * Requisitioning or issue of incorrect materials resulting in losses from wastage/delays * Failure to budget costs properly resulting in selling prices which are too low and subsequent losses * Failure to monitor actual expenditures and identify variances between actual and budget * Failure to control the transfer of finished goods to the finished goods store (manufactured items stolen, damaged or lost).

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. A costing schedule (budget) must be prepared for all products to be manufactured whether on a "job cost basis" or a "process costing basis". * These schedules should be carefully compiled by costing personnel and should contain detailed listings of all materials to be used, expected labour costs and an allocation of production overheads. * The schedules should be sequenced, dated and approved by production personnel (signature). * The schedules may be used as the source document for purchase requisitions. 2. For job orders (job costing) the details on the costing schedule * should be transferred to "job cards" (job sheet) which • are sequenced and dated • contain a list of materials to be used • are cross referenced to a customer order/quote

- are cross referenced to a materials requisition and materials issue note
- are cross referenced to the daily production schedule
- are authorised by the production manager.

* no materials should be issued from inventory without a materials requisition which has been checked against the authorised job card.
* whilst the job is in production, the job card should be held in a pending file and updated for labour hours as they are incurred.
* on completion of the job, a sequenced "transfer to finished goods form" should be made out. This will:
  - accompany the goods to the finished goods store
  - be cross referenced to the job card
  - be used to write up the finished goods perpetual inventory.
* the job cards for completed jobs should be removed from the pending file and "costed" e.g. material prices and labour costs allocated and an overhead allocation made
* all calculations should be checked by a second clerk
* the job card should then be filed numerically
* on a frequent and regular basis, supervisory staff or the production manager should sequence test the completed job card file to confirm that:
  - each card is cross referenced to a "transfer to finished goods note" and to a sales invoice.
  - missing job cards are for jobs still in the production stage.
* management should compare completed job cards to quotes and costing schedules and investigate variances.

3. For process costing
   * all process runs must be recorded on manufacturing or production schedules which are:
     - sequenced and dated
     - cross referenced to production plans
     - cross referenced to material requisitions
     - authorised by the production manager
   * as items come off the production line, a sequenced "transfer to finished goods form" should be completed for each day's production or for every say, 100 items produced. The "transfer to finished goods note" should:
     - accompany the goods to the finished goods store
     - be cross referenced to the production schedule
     - be used to write up the finished goods perpetual inventory.
   * performance reports should be used to measure performance by production shift e.g. wastage, quantities produced, damaged items.
   * completed production schedules and performance reports should be sent to "costing" for the allocation of labour and overhead costs as well as for pricing of materials. (The normal method for doing this is by the allocation of ***standard*** material, labour and overhead costs).
   * on a frequent and regular basis, management should date and sequence test the costed production schedules to confirm that:
     - the full quantity of production has been cross-referenced to "transfer to a finished goods form"
     - missing schedules are for goods still in production.
   * management should review performance reports to evaluate the production activity and should follow up on inefficiencies, wastage.
   * actual costs should be compared to standard costs and variances should be evaluated.

* the following posting should be made from signed, costed production schedules:
  - raw material costs, direct labour and manufacturing overheads to the debit of work-in-progress.
  - cost of goods manufactured to the credit of work-in-progress and the debit of finished goods.
* all casts, extentions and calculations should be checked before posting.

  Note: again this may be a computerised system but the principles described above remain the same.

8. INVENTORY COUNTS: CYCLE COUNTS AND YEAR-END COUNTS

8.1 Cycle counts

One of the common control activities which has been discussed a number of times, is the frequent comparison and reconciliation of actual assets with theoretical assets. The logic behind this is that differences can be timeously identified and investigated. Preventive measures can then be put in place to reduce the possibility of the problem which caused the differences from recurring. For example, if the quantity on hand of a (physical) item of inventory does not agree with the perpetual inventory records, there has either been misplacement of the item, the item has been lost or stolen or the perpetual inventory records are incorrect because a receipt of goods has not been recorded. Follow up may reveal that inventory is being stolen by sending out additional items when official orders are dispatched. Additional supervisory checks will then have to be put in place.

Companies which have large quantities and numerous items of inventory will normally perform what are referred to as ***cycle counts***. Cycle counts amount to the ongoing comparison of physical quantities of inventory on hand, to theoretical quantities in the perpetual inventory records. It is essential that the company operates a perpetual inventory system of quantities of inventory so that actual inventory can be compared to theoretical inventory. The procedures to be adopted to conduct cycle counts are as follows:

* the timing of each count should be planned at the start of the year, e.g. two days every three weeks, or at the end of every third month. (In very large companies such as motor manufacturers, cycle counting can be almost a daily exercise.)

* the items to be counted must be identified. There are a number of ways in which this selection can be done:
  - random samples can be selected from the perpetual inventory records
  - items which are susceptible to theft or have some other identifying characteristic can be chosen
  - high value items can be selected or
  - the entire inventory population can be divided into sections so that all items are counted at regular intervals during the year
  - a particular section of the warehouse may be chosen.

* once these matters have been settled, the physical inventory will be counted using an acceptable method of counting and sound count controls (see 8.2 below).

* the physical count quantity (actual) for each item counted will be compared to the theoretical quantity on the perpetual inventory records and all count discrepancies will be entered onto a sequenced inventory adjustment form.

* all discrepancies must be thoroughly investigated preferably by internal audit and the inventory controller.
  - results of the investigations should be recorded on the inventory adjustment form
  - the warehouse manager should review the forms and authorise the adjustments by signing the form.
  - inventory adjustment forms should be filed numerically and should be sequenced checked regularly.

* the adjustment to the records should be made by a clerk who is independent of inventory custody, receiving and issue.

* the perpetual inventory records should be reviewed periodically by senior warehousing personnel and adjustments to the records traced back to the authorised inventory adjustment form.

* an overall analysis of the discrepancies over a period should be conducted to identify any trends e.g. frequent discrepancies in a particular section of the warehouse, so that suitable preventive measures can be put in place.

8.2 The year end inventory count

For companies which do not operate perpetual inventory systems, the only way of ascertaining a closing inventory figure is to physically count the inventory and then to price it. Thus the inventory count becomes a very important activity, as mistakes in establishing the quantity and pricing of inventory can have a material effect on the financial statements (the closing inventory figure affects profit, tax, current assets etc). Companies which perform cycle counts will also conduct a year-end count and pricing exercise (perhaps to a lesser degree) also to establish an ***actual*** inventory valuation. As explained earlier in this chapter there is an endless number of inventory types and no two inventory counts are likely to be the same. However, there are some basic principles which should be adhered to, to conduct a successful count. They are as follows:

planning and preparation – this must take place timeously and should cover:

* date and time of the count.
* method of counting : how the inventory will be counted and recorded e.g. tag system, all items counted twice.
* staff requirements : how count teams are made up e.g. one person from the warehouse, one person independent of the warehouse (e.g. accounting department), how many teams are necessary.
* supervision : who will act as count controller.
* preparation of the warehouse : tidying racks, packing out half empty boxes onto racks, marking damaged goods, stacking like goods together, etc.
* drafting of warehouse floorplan to identify count areas for count teams.
* identifying all locations and categories of inventory.

design of stationery – various documents are used and they should be designed along standard stationery design principles

* inventory sheets: printed, numerically sequenced, reflect the inventory item number, category and location of the inventory in the warehouse, and have columns for first count, second count, discrepancies, and columns for prices and extentions. (In many companies, counters may need to insert descriptions etc. particularly where there is no form of perpetual inventory).
* in theory, quantities per the perpetual inventory should ***not*** be entered on the inventory sheet prior to the count (this forces counters to actually count to arrive at a quantity) but it may not be practical due to time constraints.
* inventory tags : see explanation under “documents” earlier in this chapter.
* inventory adjustment forms.

written instructions – count information and instructions should be provided (in writing) for all members directly and indirectly involved in the count. The written instructions should cover:

* the identification of count teams and the responsibilities of each member of the team.
* the method of counting to be used e.g. tags, double counts, marking counted inventory in two colours with chalk (reflecting the double count).
* identification of slow moving or damaged inventory as well as consignment inventory.
* controls over issues to and returns of inventory sheets to the count controller.
* procedures to be adopted if problems arise during count e.g. particular inventory items cannot be found, deliveries of inventory during the count.
* detailed instructions concerning dates, times, locations.

conducting the count – there are a number of variations on how the inventory count should be conducted but the following procedures should be followed:

* the count staff should be divided into teams of two, with one member of the team being completely independent of all aspects of inventory.

* all teams should be given a floor plan of the warehouse which should clearly demarcate the inventory locations for which they are to be held accountable.
* all inventory should be counted twice. One of the following methods can be adopted:
  - one member of a team counts and the other records, swapping roles thereafter and performing a second count in the same section to which they were assigned.
  - count teams complete their first counts, hand their inventory sheets back to the count controller and sign for the inventory sheets of another section, thereby doing their second counts on a section already counted by another count team.
* as items are counted they should be neatly marked by the counters. e.g. second counters should use a different coloured marker. Alternatively the tag system described under "documentation" can be used.
* where count teams identify damaged inventory or inventory in an area of the warehouse which appears unused/excessively dusty, these inventory items must be marked as such on the inventory sheets (potential write downs).
  - the contents of boxes where the packaging appears to have been tampered with, should be counted and the details noted on the inventory sheet.
* a few boxes should be selected at random in each section and the contents compared with the description on the label to confirm that the contents have not been changed/removed and the seal replaced.
* the count controller (and assistants) should:
  - walk through the warehouse once the count is complete and make sure all items have been marked twice or that the detachable portions of all tags have been removed.
  - examine the inventory sheets to make sure that first and second counts are the same and agree to the quantities recorded on the perpetual inventory if there is one.
  - instruct the count teams responsible for sections where discrepancies are identified to recount the inventory items in question.
* the count controller should obtain the numbers of the last goods received note, invoice, delivery note and goods returned note used up to the date of the inventory count.
* no despatches of inventory should take place on the date of the inventory count.
* any inventory received after the count has begun should be stored separately in the receiving bay, until the count is complete and must not be put into the warehouse. This inventory must be counted and added to the inventory sheets after the count is complete.
* the counters responsible for the count sheets should:
  - draw lines through the blank spaces on all inventory sheets, and
  - sign each count sheet and all alterations.
* the inventory controller should check that this procedure has been carried out and should sequence test the inventory sheets to ensure that all sheets are accounted for.
* count teams will only be formally dismissed once the count is complete and all queries have been attended to.

9. COMPUTERISATION IN THE INVENTORY AND PRODUCTION CYCLE

* In most companies the systems which interface with the inventory and production cycle, will be computerised and will directly affect and be affected by the inventory masterfile. For example, purchase orders will be influenced by re-order levels held on the inventory masterfile. The actual creation of the purchase order will also depend on the data held on the masterfile. For example, only items listed on the inventory masterfile can be included in the purchase order. The quantity field on the inventory field will be automatically updated by the entry of purchases or sales transactions to provide up to date information pertaining to inventory.
* The inventory masterfile is a key requirement for the effective implementation of cycle counts as discussed previously.
* Many of the control activities pertaining to the production of a manufacturing company's products e.g. creating production schedules, costing schedules, accumulating and allocating costs can be done on the system using suitable software.
* The various functions in the cycle are likely to be on the company's local area network and the basic principles applicable to computerised systems will apply, e.g. access control based upon the least privileged/need to know basis.

INVENTORY CONTROL AT PRORIDE (PTY) LTD

INTRODUCTION

As ProRide (Pty) Ltd is a wholesaler of bicycles and accessories it has a conventional inventory cycle, e.g. goods are delivered to a designated receiving depot, subjected to various checks and transferred to the storage areas. The goods are suitably protected whilst in storage until they are sold. Goods to fill sales orders are selected using picking slips, placed in a picking area once picked, checked and transferred to despatch. Internal control at ProRide (Pty) Ltd is taken very seriously and the control over inventory is no exception. The company has in excess of a thousand different inventory items which range from complete bicycles (in boxes) to small individual bicycle parts. There are also expensive items such as top quality cycling helmets, gearing systems and bicycle computers for measuring speed, distance, etc. Most of the inventory items held by the company can be easily disposed of if stolen, so theft is a major risk that the company has to respond to.

The control activities which are described below are supported by a very strong control environment in the company as a whole. For example, all employees working in the cycle are properly trained and have good product knowledge (commitment to competence). There is a clear reporting structure within the cycle and individual employees are held accountable for their actions (organisational structure and assignment of responsibility). Senior management not directly involved in the cycle are frequently in the warehouse and will, from time to time, observe the various activities which go on in the cycle, e.g. the unpacking of a container of imported bicycles (management philosophy and operating style) which sets a good example and enhances control awareness. Theft of inventory results in dismissal which emphasises the integrity and ethical values expected of all employees.

SEGREGATION OF DUTIES

1. The cycle is "broken down" into the following functions, receiving goods, custody of goods, picking of goods and despatch. In the overall context of the company, the inventory cycle is separated from the functions of initiating sales orders or purchase orders.

2. The overall responsibility for all functions rests with Reg Gaard, the warehouse manager. He is supported by Patrick Adams (warehouse foreman) who is responsible for the team of pickers.

3. As the function of receiving does not warrant the appointment of a full-time receiving clerk, the despatch controller fills both roles. He has a number of assistants who report to him, and he in turn reports directly to Reg Gaard (warehouse manager).

4. There are a relatively large number of pickers whose duties are to
   * receive goods from the receiving depot
   * pack goods into bins, boxes and onto shelves
   * pick goods to fill orders
   * pack goods into boxes for delivery (after goods have been checked)
   * keep the storage areas neat and tidy and shelves properly labelled, etc.

5. Pickers are not allowed to assist with receiving goods from suppliers or despatch to customers, and receiving/despatch employees are not allowed to pick goods.

6. Patrick Adams (warehouse foreman) plays a supervisory role over the pickers and is responsible for checking the items picked once they are placed in the picking area.

7. Both Reg Gaard (warehouse manager) and Patrick Adams (warehouse foreman) have read access to the inventory masterfile but do not have write access (segregation of custody and record keeping).

8. Reg Gaard (warehouse manager) does ***not*** have sole responsibility for authorising an inventory adjustment, final authority must come from the financial manager, Johan Els.

APPROVAL AND AUTHORISATION AND ISOLATION OF RESPONSIBILITY

1. All movements of inventory must be supported by an authorised document, e.g. the picking slip can only be generated off the (computer) system from an approved sales order, delivery notes can only be generated from an approved (signed) picking slip.

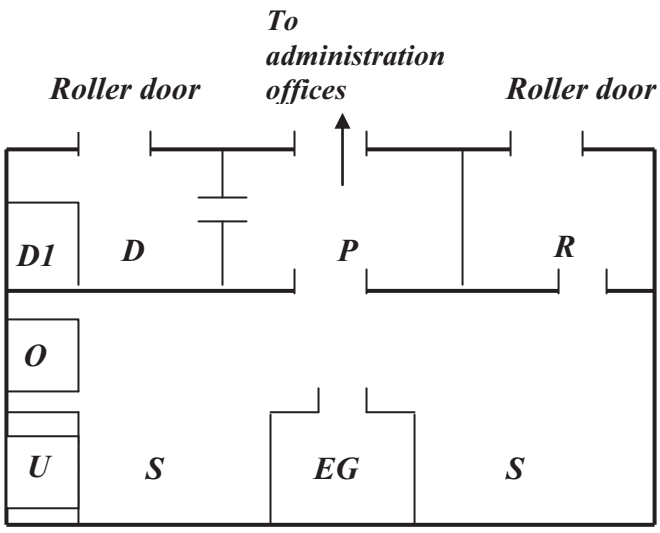
2. All adjustments to the masterfile arising out of the cycle counts must be approved by the warehouse manager and the financial manager.

3. The responsibility for receiving and despatch is isolated to the despatch controller as nobody else has access to the necessary applications and by the requirement that all relevant documentation be signed by him.

4. All employees are required to sign the document related to the procedure they have carried out to acknowledge having done so, thus isolating their responsibility for the procedure. For example
   * pickers must sign the picking slip for the goods they have picked so any mistakes or problems can be tied back to the picker
   * the warehouse foreman must also sign the picking slip to acknowledge (isolate his responsibility) for checking what has been picked before it is packed and transferred to despatch.

ACCESS/CUSTODY CONTROLS

Layout and design features of the warehouse



D	=	Despatch area
D1	=	Roadline office (delivery company)
R	=	Receiving Depot
P	=	Picking area
S	=	Storage areas
EG	=	Expensive goods store
U	=	Stairs to upper level
O	=	Warehouse staff offices

* The ProRide (Pty) Ltd warehouse is located in one large structure adjoining (by controlled access) the administration building. As can be seen from the diagram, the warehouse has distinct areas for both "despatch" (D) and "receiving" (R) of inventory. Access to and from the outside is controlled by large steel roller doors which remain locked at all times other than when despatching

or receiving takes place. The keys to these doors are under the control of Reg Gaard (warehouse manager) or Patrick Adams (foreman) at all times.

* The "despatch" and "receiving" areas are physically separated from the picking area and stores by one metre high walls with glass to the ceiling. (This method of construction which applies also to the warehouse staff offices, enables warehouse management to see what is going on within all areas of the warehouse at all times). Access to the despatch section is from the picking area, ***not*** from the storage area, which makes it far more difficult to steal inventory by "sneaking" it from stores onto a delivery van.

* The picking area (where picked goods are placed prior to final checking and despatch) is separated from the storage area by brick and glass walls but the access between the two is not controlled. This is simply for practical purposes as pickers are moving from one area to another throughout the day.

* The expensive goods store is completely secure and is locked at all times. When expensive goods need to be "picked", Patrick Adams (warehouse foreman) will unlock the store and observe the picking. Only he and Reg Gaard have access to the keys.

* The upper level is used exclusively for storing bicycles (in their boxes). A forklift is used to move boxes to and from this level. Storage of bicycles on the upper level has been done deliberately, as it makes it extremely difficult for anyone to steal a boxed bicycle.

* Access to the warehouse for warehouse staff is via the controlled access (key pad) from the main administration building. Other employees are not allowed in the warehouse.

* The warehouse is not air conditioned (the inventory does not require it!) but it is protected against fire by smoke detectors and sprinkler systems.

* Windows are kept to a minimum and are protected by grids and bars (so items cannot be thrown out of the warehouse). There is no camera surveillance as it is not considered necessary.

* Inventory is kept in clearly designated areas e.g. tyres, saddles, clothing and the various items are placed in suitably designated bins or boxes or on shelves. The item's inventory code is entered on the bin, box or shelf to facilitate accurate picking and inventory counts.

COMPARISON AND RECONCILIATION

1. Cycle counts

A very important control mechanism is the company's inventory ***cycle count*** system. The cycle counts take place every three months including year end. The counts take place on a Saturday (no interferences, deliveries, despatches). All warehouse staff, certain administration staff, the financial manager Johan Els and Brandon Nel the financial director will make surprise visits.

* The ***external*** auditors are required to be present for the entire count ***and*** to submit a full report on how the inventory count was conducted and how problems were resolved, ***direct*** to Brandon Nel during the subsequent week. (The company does not have an internal auditor.)

* Every single item is counted. Where a discrepancy arises it is immediately investigated by a team under the control of Reg Gaard (warehouse manager). This may include determining whether the item has been misplaced or checking receipts and issue records for that item since the last count.

2. Adjustments to the inventory masterfile

* If a discrepancy is not resolved and an adjustment is required to correct the perpetual inventory (theoretical inventory), a sequenced "cycle count adjustment form" is completed, and signed by Johan Els (financial manager) and Reg Gaard (warehouse manager). Details of the investigation into the discrepancy are noted on the form.

* As indicated above, Reg Gaard does ***not*** have write access to the inventory masterfile. The adjustment to the inventory masterfile is made by Dalene Burger (accounting supervisor) and a log of all adjustments is presented to the financial director (Brandon Nel) during the week subsequent to the cycle count. He will scrutinize this log, reconcile the adjustments to the supporting documentation and try to identify any trends in the discrepancies e.g. regular adjustments to tyre inventories.

  Note 1: the same adjustment procedure will take place for any inventory items found to be damaged.

  ***Note 2*:** the effectiveness of cycle counts depends to a great extent on the accuracy of the perpetual inventory records. We have emphasised in the other cycle chapters that ProRide (Pty) Ltd goes to great lengths to ensure that the information in its accounting system is correct. Because they achieve this, their cycle counts are very effective in the overall control of inventory.

PERFORMANCE REVIEWS AND THE USE OF LOGS AND REPORTS

As inventory is very much the heart of this business, Brandon Nel (financial director) spends a great deal of time analysing and interpreting inventory information.

1. Targets

To be in a position to review performance, targets are set by Brandon Nel (financial director) and Reg Gaard (warehouse manager) on an ongoing basis for activities in the inventory cycle. These include

* setting time limits for the despatch of goods from the time the sales order is put on the system. As the sales system is a real time system, management can access the sales order file at any time to determine the status of a sales order. Complaints from customers are also closely monitored.
* setting an "acceptable" margin for incorrectly picked goods (tracked through reports on the number of and reason for credit notes being issued)
* setting "acceptable" margins for goods lost, stolen or damaged (tracked through logs on inventory adjustments).

2. Information

In addition to the information extracted to determine whether targets are being met, Brandon Nel will also extract a number of reports which help with the general management of inventory, e.g.

* total inventory holding
* details of inventory in transit
* actual inventory levels for any item
* actual gross profit margins made on sales, per inventory item, per inventory category
* anticipated gross profit margins on inventory held, per inventory item per category
* quantity of items sold to date including a breakdown of those sales by distinguishing feature e.g. make and model, colour (red bicycles may sell better than blue bicycles.)
* aging of inventory on hand, highlighting inventory which has been on hand beyond predetermined limits (say 90 days).

3. Meetings

As we have mentioned on many occasions, reports and logs are not much use if there is no follow up on the information they contain. A weekly meeting between Brandon Nel (financial director), Johan Els (financial manager) and Reg Gaard (warehouse manager) is held to discuss any queries which Brandon Nel might have, arising out of the inventory information which is available to him.

CONCLUSION

The success of the control activities implemented can partially be measured in terms of the percentage of total inventory lost as a result of theft or damage and the efficiency of filling and despatching orders. At ProRide (Pty) Ltd this percentage is reasonably constant at less than half a percent of the total inventory value. Goods are despatched within 24 hours of a sales order being received.

AUDITING THE CYCLE

1. INTRODUCTION

An important part of the audit of a company's inventory cycle will be the procedures carried out to identify and assess the risk of misstatement at assertion level. This risk identification and assessment process is facilitated by carrying out procedures to obtain a thorough understanding of the client and the environment in which it operates. These procedures have been covered in some depth in chapter 7 and will not be addressed in this section of chapter 12. Once risk assessment has been carried out the auditor will be able to "assign" a level of risk to the individual assertions applicable to the account balance and thereafter plan the nature, timing and extent of ***further*** audit procedures. The objective is to devise an audit strategy and plan which reduce audit risk to an acceptable level.

2. FINANCIAL STATEMENT ASSERTIONS AND THE INVENTORY AND PRODUCTION CYCLE

The auditor's main concern with this cycle is that the asset (various categories of inventory) associated with the cycle is fairly presented in the financial statements. Earlier in the chapter we indicated that any material misstatement in the inventory balances will have a significant effect on fair presentation of both the statement of comprehensive income and the statement of financial position.

2.1 The assertions which apply to the inventory account balance as follows:

rights: the company holds or controls the rights to all inventory reflected in the financial statements (any encumbrances must be disclosed)

existence: all inventory included in the account balance actually existed at the reporting date (inventory is not overstated by the inclusion of fictitious items)

completeness: all inventory to which the company has the rights of ownership, is included in the financial statements. All inventory that should have been recorded, has been recorded.

valuation and allocation: inventory is reflected in the financial statements at an appropriate amount (carrying value) (this means that appropriate adjustments have been made to comply with the requirement that inventory be presented at the lower of cost or net realisable value).

2.2 Assertions pertaining to presentation and disclosure

In addition to the assertions applicable to the inventory balance identified above, the directors are also representing (asserting) that the presentation and disclosure of all matters pertaining to the balances in this cycle are ***complete*** in terms of the applicable financial reporting framework, e.g. IFRS, have been correctly ***classified*** and ***accurately*** presented and disclosed in an ***understandable*** manner.

3. IMPORTANT ACCOUNTING ASPECTS – IAS 2 INVENTORIES

This International Accounting Standard is very important as it provides the company and the auditor with definitions and the basic requirements for the methods with which inventory can be valued and how it should be presented and disclosed in the financial statements.

3.1 Definitions

* ***Inventories*** consist of:
- assets held for sale in the ordinary course of business (finished goods and goods purchased for resale)
- assets held in the process of production (work-in-progress)
- materials or supplies to be consumed in the production process (raw materials)

* ***net realisable value*** is the estimated selling price in the ordinary course of business less the estimated costs of completion and the estimated costs necessary to make the sale.

3.2 Inventory should be presented at the lower of cost and net realisable value

This acknowledges the important principle that the asset (inventory) should not be carried at an amount greater than is expected to be realised from the sale of the asset. Such a situation could arise where:

* inventory has been damaged
* inventory has become obsolete
* the selling price has declined to below the cost of the asset due to a drop in demand.

This has a direct effect on the auditor who will need to perform procedures to determine whether inventory has been written down adequately to reflect any or all of the above.

3.3 Cost of inventories

The cost of inventories should consist of :

* all costs of purchase including import duties and transaction costs that are not reclaimable (VAT is a reclaimable transaction cost), transport costs incurred in the acquisition of materials, goods for resale, etc.
* costs of conversion e.g. direct labour and production overheads
* costs incurred in bringing the inventory to its present location and condition, e.g. costs incurred in designing a product for a specific customer.

It is also important to note that the following should be ***excluded*** from the cost of inventory:

* storage costs (unless these costs are necessary in the production process before a further production stage)
* administrative costs (other than those incurred in bringing inventory to its present location and condition)
* selling costs.

The auditor will need to be satisfied that these three categories of cost have been written off as expenses and not included in the cost of inventory.

3.4 Cost of manufactured goods

* the allocation of overheads to the cost of manufactured inventory must
  - include only fixed and variable ***production*** overheads
  - be based on normal capacity and must
  - be allocated on a systematic basis which is reasonable
* abnormal amounts of wasted material, labour or other (abnormal) production costs should be excluded.

Note: the three exclusions listed in 3.3 also apply to manufactured inventory.

3.5 Cost formulae

IAS 2 permits the adoption of three cost formulae:

* specific identification
* weighted average
* FIFO

It is important that the auditor understands the application of the cost formulae adopted by the company as it directly affects the measurement of cost of sales and the valuation of inventory at the financial year-end, e.g. the use of the FIFO formula assumes that the items which were purchased first, are sold first. Hence those that remain in inventory at year end will be valued by working backwards from the most recent price. Using weighted average, the valuation of the remaining inventory would be based on a weighted cost for that inventory.

Note: In addition to measuring the cost of inventory in terms of the actual cost incurred, IAS 2 also allows the use of standard costs and the retail method. However, the value of inventory arrived at by using these methods will only be acceptable for use in the financial statements where the cost determined approximates actual costs. Where standard costs are used, the company will end up with inventory valued at standard as well as some variances. It stands to reason that if the standard is wrong the carrying value of inventory will either be understated or overstated. The principle that inventory be presented at the lower of cost and net realisable value still holds, and if there is a problem with the "standard" cost, it must be addressed by scrutiny of the variances relating to the inventory. The following points are relevant:

* only variances which relate to inventory actually on hand at year-end can affect the value of that inventory (some of the variances will relate to inventory already sold).
* variances which are a result of incorrect standard setting should be debited or credited to inventory and cost of sales to approximate actual cost (to comply with the requirements of IAS 2).

For example if at reporting date, a company has an adverse material price variance (i.e. goods purchased at a price higher than standard), must the variance be written off as an expense or can it be added to the cost of inventory (which is at standard)? Any portion of the variance pertaining to inventory which has been manufactured or sold, must be written off. If the remaining portion of the variance arises because the standard was incorrectly set, the cost of inventory should be adjusted to arrive at the true cost. What about a situation where the standard is correct but a variance has arisen as a result of an abnormal price having been paid for material? For example, assume that a shortage of the material has temporarily pushed up the price and that such material was purchased just before year-end and will only be used in the new year. In terms of IAS 2, the standard cost can be used if it approximates actual costs. It would seem therefore that the price variance arising from this abnormal cost would have to be added to the cost of inventory at standard for financial reporting at the year-end.

3.6 Pricing of imported inventory

* the exchange rate at which purchased inventory must be recorded is the rate at transaction date (not payment date)
* even if the exchange rate is different at the financial year-end, ***no*** change is made to the value of inventory at year-end.

4. FRAUD IN THE CYCLE

4.1 Fraudulent Financial Reporting

As mentioned earlier in the chapter, inventory presents the directors with an effective opportunity for reporting fraudulently by manipulating the inventory balance. The inventory balance is used in the calculation of profit and is used in the statement of financial position and therefore its manipulation can have a pervasive effect, e.g. on profits, important ratios and earnings per share. The directors may

* ***include fictitious inventory*** (existence). This will increase profit and current assets and improve related ratios.
* ***understate the writedowns of inventory for obsolescence, damage etc*** (valuation). This will have the same effect as above.
* ***exclude inventory which should be included and/or overstate inventory writedowns*** (existence and valuation). This will have the opposite effect, and will only arise when the directors are attempting to make the company look less "valuable" than it is, e.g. if they are planning a management buyout. This approach could also be part of an overall scheme to evade taxation.

There are hundreds of different ways of including fictitious inventory. As all directors know that the auditor will conduct ***physical*** tests on inventory, many inventory frauds require quite intricate planning and a lot of deception to create the "illusion" of inventory.

Generations of auditing students have learnt about the "Great Salad Oil Swindle" which, although it occurred over 50 years ago, illustrates how simple it is to hoodwink intelligent people (including auditors!), with schemes and scams to falsify inventory, and to what lengths directors might go, to overstate inventory.

In this fraud, Tino De Angelis, founder of Allied Crude Vegetable Oil Refining Corporation of New Jersey, built up a huge edible oil empire. By the late 1950s, the company supplied more than 75% of the USA's edible oil exports (over 100 million dollars per annum). The company used existing inventories as security for the finance necessary to fund futures deals, and to effectively control world prices. Existing oil inventories were counted on a ***weekly*** basis and the finance for the futures deals was advanced by the banks on the basis of documents certifying that the oil inventories existed. The financiers, who were present at the inventory counts were mislead in a number of ways, including:

* interconnecting of oil tanks so that oil could be pumped from one tank to the next as the count proceeded.
* some tanks had a thin "pipe" full of oil, below the inspection hatch at the top of the tank, the remainder of the tank being empty. When the measuring rod was inserted to check the level of oil in the tank, it obviously measured "full" as it had been inserted into the thin pipe of oil.
* some tanks contained seawater, with only a small false chamber welded to the top of the tank containing oil.

These fraudulent activities were eventually discovered after oil prices collapsed due to De Angelis's over manipulation of the futures market. The financiers called in the credit extended for the futures deals and, when the company could not pay, they sought to liquidate the inventory which was certified as their security, only to find that most of it did not exist!

As pointed out earlier, employees who misappropriate inventory usually need to hide the theft from the management, internal auditors and the external auditors.

Likewise where management are attempting to report fraudulently, they will probably need to get the inventory records and physical inventory to agree. Where inventory which has been stolen or never existed has been included in the inventory records, it can be "reconciled" with physical inventory by

* including empty containers, e.g. boxes, in the count
* hollow stacking e.g. surrounding empty containers with full containers (hoping those testing physical inventory will not "unstack" the containers to check the contents)
* attaching an empty container to the shelf to make it appear heavy and thus appear to be full
* packaging bricks etc in proper inventory packaging
* re-packing defective or second hand goods to look like new inventory
* altering (increasing) the "quantity on hand field" inventory count sheets ***after*** the count
* including inventory which is not what the records indicate it is e.g. stealing genuine Nike T-shirts or Oakley sunglasses and substituting them with cheap "look-alikes"
* borrowing inventory from a related party just for the inventory count
* having recently sold goods returned under false pretences for the purpose of the inventory count e.g. a motor vehicle
* double counting e.g. inventory in transit, multiple inventory locations
* obtaining false 3rd party confirmations from agents or related parties
* including consignment inventory belonging to others as company inventory
* manipulating year-end "cut-off" of purchases and sales
* including goods received in the physical inventory count but not in the records
* pre-invoicing and including the goods sold in the physical count as well.

4.2 Misappropriation of assets

In this cycle this normally simply amounts to straightforward theft! This presents the perpetrator with two challenges. Firstly how to get the goods and secondly how to hide the theft.

How to get the goods will depend on

* the nature of the goods, e.g. it is much easier to steal a small valuable item than a large "difficult to move" item.
* the physical control over inventory e.g. limited exits, surveillance cameras, etc all make it more difficult.
* the extent of division of duties e.g. if a warehouse employee prepares documentation for despatch and picks and packs the goods for despatch , theft becomes much easier.
* the frequency of physical and theoretical reconciliations of inventory i.e. inventory counts. The more frequent and thorough these counts are, the harder it is to steal without being caught.

* the controls in the other cycles which directly affect the inventory cycle, e.g. controls over receiving goods (acquisition cycle) and controls over despatching goods (revenue cycle).

As indicated earlier, hiding the theft is also part of misappropriating inventory. There are numerous ways of doing this, but the best opportunity is presented when there is a lack of division of duties between record keeping for inventory and custody of inventory. If the perpetrators of the theft are able to amend the inventory records or issue documents such as goods returned notes, it will be simple for them to cover the theft. The situation will be exacerbated where the control environment is weak.

5. TESTS OF CONTROLS AND SUBSTANTIVE PROCEDURES

5.1 Tests of controls

The auditor's main focus is normally on substantive testing of the inventory balance. However, some tests of controls will be carried out and will centre around the following:

* ***observation*** of the inventory count.
* ***inspection*** of reconciliations and cycle count amendment forms for cycle counts carried out during the year, to determine frequency and materiality of discrepancies and how they were resolved and for authorising signatories.
* ***observation*** of warehouse controls to determine the effectiveness of:
  - access control, (custody and safekeeping)
  - controlling inventory movement.
* ***inspection*** of records controlling inventory movement e.g.:
  - a sample of requisitions and materials issue notes for:
    - authorising signatures and
    - cross referencing to job cards
  - a sample of inventory movements per the perpetual inventory records to "transfers to finished goods notes".
* ***inquiry*** of production and warehousing as to what control procedures they actually perform.

5.2 Substantive procedures

Many of the tests which are carried out as tests of controls will be dual purpose tests and will supply some evidence relating to the accuracy of the inventory records. The auditor's objective is to satisfy himself that the quantities of inventory at year end are correct, and that the cost formula has been correctly applied. In addition, the reasonableness of any write downs of inventory must be evaluated. All of this will be achieved by the application of substantive audit procedures on the year end inventory account balances.

The performance of year-end procedures is usually broken down into two distinct phases, namely:

* attendance at the year-end inventory count (mainly ***existence***, but some evidence of ***completeness*** and ***valuation*** is gathered).
* the subsequent audit of the carrying value (***valuation, rights*** to the inventory and the ***presentation and disclosure*** of inventory).

5.2.1 attendance at the inventory count is both a test of controls and a substantive procedure. The auditor will be gathering evidence as to the effectiveness of the control procedures put in place to establish the quantity of inventory actually held (test of controls). At the same time the auditor will be gathering substantive evidence about:

* the ***existence*** of the quantity of inventory recorded by testing from the records to the physical inventory.
* the condition of inventory (***valuation***) by inspecting and looking for damaged/obsolete items, as well as evidence of slow moving inventory.

* the ***completeness*** of inventory by testing from the physical inventory to the inventory records.

5.2.2 the subsequent audit procedures i.e. after the inventory count, will be substantive in nature.

5.2.3 another important procedure which is carried out at the inventory count will be the recording of the last document numbers for all documents used, e.g. goods received notes, issue notes, delivery notes etc, to facilitate "cut off" testing. From an inventory perspective, it is important that the ***recorded*** movement of inventory matches the ***physical*** movement of inventory up to reporting date.

5.2.4 a list of goods received notes numbers which have not been matched to suppliers invoices at the year-end should be obtained. This will be used later for testing the completeness of creditors.

5.3 Inventory count attendance

As attendance at the inventory count is an important procedure, we will deal with it separately:

5.3.1 ***prior to the inventory count*** the auditor should:

* liaise with the client about date and times of the inventory count.
* confirm all locations at which the client holds inventory (by enquiry, reference to prior year workpapers) and if necessary visit the locations.
* perform administrative planning e.g. organize audit staff to attend.
* obtain and review a copy of the written instructions given to the client's count teams (see "inventory counts" page 12 earlier in the chapter).
* enquire as to whether the client has any inventory which should ***not*** be included in the count e.g. consignment inventory, inventory already invoiced but not yet delivered or collected. Establish how this inventory is physically identified.
* brief the audit staff allocated to the count on their responsibilities.

5.3.2 ***during the inventory count*** the auditor should:

* observe inventory taking procedures to ensure that the client's written instructions are adhered to.
* walk through the warehouse and identify inventory which is obsolete or damaged or appears to be slow moving e.g. dusty, old packaging etc The inventory number, description, location and quantity should be recorded on a workpaper and traced to the inventory sheets to confirm that these items have been marked as damaged/obsolete.
* conduct test counts on the inventory in the warehouse in both directions, making sure all sections and categories are tested:
  - from inventory sheets to physical inventory (***existence***).
  - from physical inventory to inventory sheets (***completeness***).
* resolve discrepancies in test counts before conclusion of the count by recounting with the client staff and confirming that amendments are made to the inventory sheets where necessary.
* test the numerical sequence of the inventory sheets both before and at the conclusion of the count to ensure that all inventory sheets are accounted for.
* confirm by enquiry of inventory counters and inspection of the inventory sheets that inventory which should ***not*** be included in the client's inventory, has been excluded.

5.3.3 ***at the conclusion of the count,*** the auditor should:

* inspect inventory sheets to confirm that:
  - lines have been drawn through blank spaces (so that items cannot be added),
  - alterations /corrections have been signed, and
  - inventory sheets have been signed by the counters responsible.
* create audit records in respect of the inventory count attendance by:
  - taking copies of all inventory sheets (hardcopy or digital)
  - recording observations as to the client's count procedures
  - recording results of all test counts preformed by the audit team
  - recording any damaged, obsolete or slow moving inventory.
* record cut-off numbers for all documents used in the inventory and production cycle.

* compile a list of goods received notes which have not been matched to supplier invoices.

The next stage in the year-end audit of inventory can commence at any time depending on the reporting deadline for the audit. The important point is that the inventory count must have provided sound evidence that the quantities and description of inventory which was on hand at reporting date, are accurate. The client will now be in a position to make any adjustment necessary to the perpetual inventory records and "price" the inventory on hand.

6. *POST INVENTORY COUNT PROCEDURES* (valuation, rights, completeness, presentation and disclosure)

6.1 Assertion - rights - the company holds or controls the rights to the inventory

* enquire of management as to whether any inventory is held on consignment for other parties.
* obtain a listing of inventory of goods in transit at the financial year-end and inspect relevant orders/contracts to determine whether ownership has passed to the client by scrutiny of the terms of purchase e.g. FOB, CIF.
* establish whether inventory is in any way encumbered (e.g. offered as security) by
  - discussion with management
  - inspection of bank confirmations
  - review of directors' minutes
  - review of correspondence/contracts with suppliers and credit providers.
* when performing the pricing procedures for the valuation assertion (see below) inspect invoices to ensure that they are made out to the client (this will also have been done when testing purchase transactions).

6.2 Assertion – valuation and allocation - inventory is included in the financial statements at appropriate amounts

To establish the value of inventory, the client will have to multiply the quantities confirmed at the inventory count by the cost price of the item, using the correct cost formula. Once this is done the allowance for inventory obsolescence must be established.

6.2.1 ***arithmetic accuracy***

* compare the quantities of inventory items on the auditor's copies of the inventory sheets to the client's priced inventory sheets (to confirm that the client has not altered the quantities).
* test the arithmetical accuracy of the inventory sheets by reperforming all extensions (quantity x cost) and casting the extension column (total inventory value).
* review inventory sheets for any negative "inventory item values" (should not be any).
* compare the total inventory value per the inventory sheets to the general ledger and trial balance.

6.2.2 ***pricing inventory purchased locally***

* using the sample selected for inventory items which were test counted at the inventory count (or another sample):
  - trace to relevant suppliers invoices to establish whether the correct purchase prices have been used in obtaining the cost in terms of the cost formula used by the company,

    e.g. for FIFO, if there are 10 items on hand, and the most recent invoice was for 8 items at R200 each and the invoice prior to that was for 12 items at R190 each, the 10 items on hand would be valued at

    8 x R200 - R1600
    2 x R190 - R380
  - reperform the weighted average calculation (if this basis is used by the client) and compare result to the weighted average price used by the client,

- by enquiry of the costing clerk and inspection of invoices from transporters, establish that relevant carriage costs have been included in unit cost calculations.

6.2.3 ***pricing imported inventory purchases***

* for a sample of imported high value items, obtain the relevant suppliers invoices /shipping contracts and costing schedule, and reperform the unit cost calculations for the sample of imported items and verify that:
  - the correct exchange rate was used to convert the foreign currency to Rands (rate at date of transaction should be used. This rate should be confirmed by enquiry of a financial institution.)
  - the appropriate import and customs duties and shipping charges were included (obtained from shipping agents invoices)
  - the allocation of the above costs to the individual inventory items purchased is reasonable, and accurately performed.

Note: a company which imports inventory will usually have a "costing schedule" which provides the details of how the cost of the imported goods was arrived at. The auditor would use this as the basis for auditing unit cost. Amounts used in the calculation would be traced to supporting documentation e.g. shipping agents invoice, suppliers invoice.

Note: for the performance of pricing tests, it may be necessary to trace suppliers invoices etc prior to the most recent ones. The goods actually on hand may have been purchased on two or three occasions at different prices.

6.2.4 ***pricing manufactured goods***

* enquire of appropriate personnel and inspect documentation used in the costing exercise to gain an understanding of the costing method used.
* determine whether it is consistent with prior years and remains appropriate for the business.
* where a standard costing system is used
  - determine the appropriateness of the standard setting process (including adjustments to standards) by discussion with management and inspection of budgets, historical records.
  - evaluate the treatment of variances at year-end to confirm in particular that the value of inventory has not been inappropriately increased.
* by inspection of the costing schedules and supporting documentation
  - agree description of materials used and prices thereof
  - agree labour costs to payroll records (rates and hours charged)
  - confirm that the allocation of overheads includes only fixed and variable production overheads and
  - is based on normal capacity and
  - is on a systematic basis which is reasonable.
* confirm that costs which do not qualify as costs of conversion have not been included e.g.
  - administration overheads
  - selling expenses
  - abnormal amounts of wasted material, labour or other production costs.
* confirm that under and over recoveries of production overheads are correctly treated in terms of IAS 2 (through the statement of comprehensive income).
* reperform all casts and calculations.

Note: the same procedures will need to be adopted to value work-in-progress at reporting date. However, there is the additional problem of establishing the stage of completion of the goods being produced. It is possible that there will be numerous items still in production and at various stages in production. Consider a motor assembly line which may have 500 vehicles on the production line at the "close of business" on reporting date. For financial reporting purposes the value of materials, labour and overheads expended on those cars in their various stages of completion, e.g. engine assembly, trim, paintshop etc, at reporting date will have to

be calculated. It is the client's responsibility to produce a schedule of work-in-progress and the audit thereof will be performed using conventional tests of controls (to test the way in which the client "puts the figure together"), and substantive tests.
In addition, complex work-in-progress may require that reliance be placed by the auditor on the work of an expert or internal audit. This is covered in chapter 16.

6.2.5 ***lower of cost/net realisable value***

- using a sample (possibly one already extracted) verify the selling price of inventory items by:
  - reference to sales lists
  - reference to the most recent sales invoice for the particular item.
- compare sales prices on invoices for a small sample of sales made in the post reporting date period to the cost prices on the inventory sheets. This provides evidence of the most up to date realisable value.

6.2.6 ***inventory obsolescence allowance***

- discuss with management:
  - the process used to determine the obsolescence allowance and evaluate the process for reasonableness and consistency with prior years, e.g. is a fixed percentage used each year (only acceptable if there is strong historical evidence to support it) or is a detailed analysis carried out?
  - any procedures in place for the approval of the final allowance, e.g. is the allowance approved by the financial director after consultation with the warehouse manager?
  - any specific events which may have occurred during the year which may have an impact on the allowance – e.g. a flood may have damaged some inventory items.
  - any specific inventory items which may already be obsolete (or soon will be) and how this has been recognised in calculating the allowance for obsolescence.
- perform analytical procedures to give a general overview as to the reasonableness of the allowance by comparison of current year figures and/or ratios to prior year figures/ratios e.g.:
  - the allowance itself
  - the allowance as a percentage of total inventory
  - inventory turnover ratio
  - days inventory on hand
- assess indicators of obsolescence problems such as no recent sales or purchases of particular items, products which have reached their sell by dates in the post reporting period, or correspondence relating to inferior products supplied to customers.
- reperform the aging of inventory by tracing back to source documents.
- compare allowances raised in prior years to actual write offs in subsequent years (to determine "accuracy" of management's allowances).
- review working papers from year-end test counts to ensure that inventory items identified as damaged/obsolete/slow moving have been included in the allowance.
- reperform any calculations of the inventory obsolescence allowance and discuss the reasonableness of the allowance in terms of evidence gathered, with management.

6.3 Assertion – completeness and existence (all inventory which should have been recorded, has been recorded, and inventory included in the statement of financial position, actually exists, it is not fictitious)

The primary evidence for these two assertions is gathered when attending the inventory count as described earlier. Additional but superficial evidence will be provided by analytical review. "Cut off" tests performed when auditing the revenue and receipts cycle and the acquisitions

and payments cycle will provide evidence that all inventory which was purchased, has been included and inventory which had been sold, has been excluded.

6.4 General – all assertions

* perform an overall analytical review of inventory by comparing current year figures and ratios with the corresponding figures of prior years e.g.:
  - total inventory
  - total inventory by category or location or source (local/imported)
  - inventory as a % of current assets, total assets.
* include reference to inventory, particularly the allowance for obsolescence, in the management representation letter.

6.5 Assertions pertaining to presentation and disclosure

* The auditor must inspect the financial statement disclosures and consider whether
  - they are complete in terms of the relevant reporting framework e.g.
    - encumbrances on inventory (security)
    - accounting policies
    - cost formula
    - cost of goods sold
  - they are consistent with evidence gathered on the audit
  - amounts, facts, details etc are accurate and agree with the evidence gathered
  - any classification of the information disclosed is appropriate e.g. W.I.P, finished goods, raw materials
  - the wording of the disclosures is clear and understandable e.g. the circumstances that led to a reversal of impairment.

7. THE USE OF AUDIT SOFTWARE (SUBSTANTIVE TESTING)

When the client has a computerised system and suitable audit software is available, extensive use can be made of it to enhance the audit of inventory. What can actually be done by the software will depend on the information which is available on the masterfile. Normally the inventory masterfile will contain, at least, the following fields:

- inventory item number
- inventory description
- category
- location
- imported/local
- approved suppliers
- quantity on hand
- unit selling price
- unit cost
- date of last receipt and GRN number
- date of last issue and document number
- inventory item value (quantity x unit cost)

The following appendices provide a simple illustration of how audit software can be used to assist in the audit of inventory.

Appendix 1. Inventory Masterfile
2. Procedures using audit software.

A SCHEDULE OF INDIVIDUAL INVENTORY ITEMS EXTRACTED FROM THE INVENTORY MASTERFILE OF DO-IT (PTY) LTD AT 31 MAY 0003

Item Code	*Description*	*Supplier Code*	*Quantity*	*Unit Cost* *R*	*Value* *R*	*Selling Price* *R*	*Date of last sale month/year*	*Date of last Purchase month/year*	*Quantity sold year to date*
T0101	Bosch Electric Drill	DR649F	18	320	5760	975	5/0003	2/0003	36
T0301	Dekker Router	PQ417	14	425	5950	1025	8/0002	6/0003	2
G041	Wheelbarrow	LG7	104	108	11232	196	5/0003	4/0003	712
H415	Metal Ladder	CL413	-3	140	-420	392	3/0003	11/0002	47
H436	Basin Set	BR200	14 62	490 545	6860 33790	740 740	5/0003	3/0003	226
T0491	Flatbed planer	PQ472F	8	4320	34560	6500	11/0002	6/0002	1
G093	Trimmer	WP293	32	1140	36480	1000	1/0002	4/0002	0
H481	Geyser 200L	CG321	-45	-630	28350	1960	3/0003	1/0003	40
T461	Arc Welder	YP731F	4	8209	65672	12450	6/0002	3/0001	2
G126	Irrigator	WW373	0	1299	0	1850	2/0003	4/0003	10
T = Tools G = Garden H = Household F after Supplier Code = Foreign Supplier Unit cost is Fifo (Masterfile has been simplified)									

PROCEDURES THAT MAY BE CONDUCTED ON THE INVENTORY MASTERFILE OF DO-IT (PTY) LTD USING AUDIT SOFTWARE

PROCEDURE	***ASSERTION***	***EXAMPLE/NOTES***
1. Stratify population by item category and value. (The same stratification could be done for imported/local items)	General	Can be used for • planning inventory counts • analytical procedures • selecting samples
2. Scan the entire masterfile and produce reports of "error conditions" for follow up		
2.1 blank fields	-	
2.2 duplicate item codes	existence	nil
2.3 negative quantities or negative unit costs	valuation-cost	H415
2.4 negative quantities and negative unit costs	valuation-cost	H481 (note value field)
2.5 quantity field is zero but date of last purchase is more recent than date of last sale	completeness/valuation-cost	G126
2.6 items with amounts in the value field but 0 in the quantity field	valuation-cost	nil
2.7 date of last sale or last purchase is after year-end	existence / completeness	T0301
3. Select samples		
3.1 pricing	valuation-cost	1. random 2. high value 3. high quantity 4. imported 5. old inventory
3.2 inventory count	existence, valuation (cost and write down)	
4. Reperform		
4.1 quantity x unit cost calculation and compare to value field for each item (report of differences)	valuation-cost	T461
4.2 cast of value field for entire file		
5. Analyse inventory masterfile by extracting listings of		
5.1 inventory items for which unit cost exceeds selling price	5.1 to 5.4 provide evidence for determining write downs (valuation)	G093
5.2 inventory items for which date of last sale is say, 9 months prior to year-end and date of last purchase is within two months of year-end		TO301
5.3 inventory items for which date of last sale and date of last purchase are say 9 months prior to year-end		G093, T461
5.4 inventory items where quantity on hand is say 5 times greater than "quantity sold to date"		T0491, G093

CHAPTER 13

PAYROLL AND PERSONNEL CYCLE

CONTENTS

		Page
ACCOUNTING SYSTEM AND CONTROL ACTIVITIES		
1.	Introduction	13/2
2.	Characteristics of the cycle	13/2
3.	Objective of this section of the chapter	13/3
4.	Basic requirements for any wage system	13/3
5.	A narrative description of a manual wage system by function	13/4
6.	Documents used in the cycle	13/5
7.	Flow charts for a manual wage system	13/6
8.	Computerisation of the payroll cycle	13/14
	A narrative description of a computerised (wage) payroll system by function	13/16
9.	Salary systems: manual and computerised	13/29
10.	The role of the other components of internal control in the payroll system	13/29
THE PAYROLL AND PERSONNEL CYCLE AT PRORIDE (PTY) LTD		13/31
AUDITING THE CYCLE		13/37
1.	Introduction	13/37
2.	Assertions	13/38
3.	Further audit procedures	13/39

ACCOUNTING SYSTEM AND CONTROL ACTIVITIES

1. INTRODUCTION

The payment of salaries and wages is an integral part of any business, and as it is a cycle which results in an outflow of funds from the business, it is extremely important that the accounting system and related control activities are sound, so as to prevent what can amount to significant misappropriations of funds. The major differences between salaries and wages are:

* salaries are expressed as a fixed monthly amount whilst wages are calculated based on the hours worked by the employee. Thus salaried employees are seldom required to "clock" in and out.
* salary earners are not usually paid for working overtime, whilst wage earners are usually paid overtime and at an increased hourly rate.
* salary earners are usually paid by direct transfer of funds into their bank accounts, whilst wage earners in some situations are still paid in cash. However payment of wages directly into the employee's bank accounts is also common practice.
* salaries are paid monthly whilst wages are paid weekly or every two weeks. In larger organisations there is a distinct trend towards paying hourly paid employees monthly (or four week blocks) due to the fact that it is more efficient and cost effective to produce a monthly payroll than to produce a weekly or bi-weekly payroll.

2. CHARACTERISTICS OF THE CYCLE

2.1 Major expense

The cycle controls what is to most businesses, a major expense.

2.2 May involve cash

Although many businesses are moving away from using cash to pay wages by making payments directly into employees' bank accounts, there are businesses (usually smaller) which pay wages in cash. This presents a risk to both the business and its employees, e.g. theft from the company, armed robbery of employees.

2.3 Susceptibility to fraud

Salary and wage frauds are not uncommon. The reasons for this are reasonably straightforward:

* in businesses which pay wages in cash, the presence of cash may be very tempting to some employees. If there is a poor control environment and inadequate supervision/division of duties, as may be the case in many smaller entities, the relative ease of misappropriating cash makes it very tempting to do so.
* the "rewards" of perpetrating a payroll fraud can be considerable, for example, if a company has a large workforce which fluctuates around say, 3000 employees, it will probably be reasonably easy to include an additional 15 or 20 fictitious workers on the payroll if controls are not very strict. This could generate substantial "cash" for the perpetrators, enough to bribe or tempt employees in the payroll and personnel departments, to collude with each other. It is not that uncommon to read about frauds involving the inclusion of "ghost workers" (fictitious employees) on provincial or government payrolls and there is little doubt that it also happens in the private sector.

The introduction of controls such as biometric readers to control the recording of hours worked by employees, and payroll software that requires a genuine employee tax number and identity number (mandatory fields) to process a wage or salary, make it far more difficult to create a fictitious employee. However, it is important to realise that in the context of a wage or salary system, a fictitious employee does not have to be a non-existent person. He can be a "real live" person with a genuine bank account, tax number, etc, but who does not actually work at the company. Obviously, the problem with this situation for the perpetrators of the fraud is that there would be an audit trail directly to the "fictitious employee" if the fraud was detected, but in an entity with thousands of employees, detecting fictitious employees may not be that easy, particularly as there is likely to be collusion amongst employees involved in the fraud.

3. OBJECTIVE OF THIS SECTION OF THE CHAPTER

Our objective in this section of the chapter is to provide you with the necessary information on how wage and salary systems work. Our approach is to provide a thorough knowledge of a manual system and then to illustrate how things may change as computerisation is introduced into the system. Remember that computerisation does not change what is required of the system, e.g. record hours worked, calculate amounts to be paid, but it does change how these things are done.

4. BASIC REQUIREMENTS FOR ANY WAGE SYSTEM

As in most cycles there is no "one system fits all" and, on your way to becoming an accountant or auditor, you will come across numerous variations in payroll systems. You will find smaller systems which are manual, systems that are partially computerised as well as systems which are extensively computerised. How the entity decides on a suitable wage system will be determined by the circumstances or characteristics of the business such as:

* ***the number of wage earning employees*** e.g. a large manufacturing company with say, 5 000 employees will need to computerise all aspects of its wage system and not pay its employees weekly. It would be totally impractical to keep employment records, record time and prepare a payroll for 5 000 employees manually. Conducting a physical payout (as opposed to transferring money directly into the wage earner's bank account) would also be impractical and dangerous.

* ***the nature of the business*** e.g. a large distribution/trucking company in KwaZulu Natal has around 300 drivers, 65 warehousing employees and 40 workshop personnel. As the drivers are away on trips for long periods, they keep their own time records of hours worked on handwritten, pre-printed schedules which are subsequently partially manually processed. The warehouse employees wage system is fully computerised (biometric timekeeping with automatic download of hours worked, paid by EFT). Because the workshop personnel work erratic hours (to keep the trucks on the road) and because the workshop is some distance from the warehousing access point, their wage system is a manual clock card (batch controlled) system but they are paid by bank transfer.

* ***the requirements of the workforce*** e.g. the wage earners may not have bank accounts or may specifically want to be paid in cash as it may be more convenient for them. (Note: some companies make it a condition of employment that all employees have bank accounts.)

* ***the location of the business*** e.g. businesses operating in remote rural areas may be forced to pay wages in cash due to the lack of banking facilities accessible to an often immobile workforce.

* ***crime*** e.g. the personal safety of employees (from muggings and violent theft) may force the company to pay wages into employee bank accounts rather than have cash wage payouts.

However, all wage payroll systems will have the same basic functional requirements which can be broken down as follows:

4.1 Personnel (Human Resources)

* There must be an individual or department which looks after the human resource aspects of the labour force, e.g. maintaining personnel records, assisting with appointments/dismissals, etc.

4.2 Timekeeping

* There must be a method of accurately recording all time worked by hourly paid employees.

4.3 Payroll preparation

* Amounts payable to employees must be calculated and supporting documentation must be created.

4.4 Payment preparation and payout

* Amounts owed to employees must be paid to them either in cash or by transfer into their bank accounts.

4.5 Deductions: Payment and Recording

* Amounts which have been deducted from employees' earnings must be paid over to the respective parties, e.g. PAYE paid to SARS.

5. A NARRATIVE DESCRIPTION OF A MANUAL (WAGE) PAYROLL SYSTEM BY FUNCTION

The following paragraphs present a brief narrative explanation of each function as listed in 4.1 to 4.5 above.

5.1 Personnel (human resources)

* as the name suggests, the personnel department deals with all aspects of the human assets of the company. The department should be skilled in such things as recruiting, counselling, negotiating and labour law, as they will be involved in all of these things on an ongoing basis. On matters more specific to the cycle, they will be responsible for keeping detailed records of all employees, executing the hiring and dismissing of staff and ensuring that pay rates and changes thereto, are correctly and promptly implemented. Independent employee record keeping is very important as it provides theoretical proof of the existence of employees and would certainly discourage the practice of including fictitious or "dummy" employees on the payroll. It is also essential for ensuring that individual employees do not fall foul of the tax regulations.

5.2 Timekeeping

* this function is required so that an accurate record of the hours for which an employee must be remunerated, is obtained so that the employee's pay for the period can be calculated.

* there are various methods that can be used for keeping time manually, e.g. the foreman ticks his employees off on a list as they arrive and leave, or the employee fills in a preprinted timesheet recording his time of arrival and departure. The most common method of "manual" timekeeping remains the clockcard. This is a thin cardboard card which is put into a timeclocking device by the employee when he arrives or leaves the workplace. The time of entry or exit is stamped onto the clockcard for each day. At the end of the wage period, a wage clerk uses the stamped clockcard to calculate the hours worked by the employee, both normal and overtime, for the wage period.

5.3 Payroll preparation

* in this function, the amount which each wage earner is to receive, is calculated. The gross amount is calculated by multiplying the hours the wage earner has worked, split between normal time and overtime, by the wage rate applicable to the grade or level at which the employee is engaged. The overtime rate will be higher than the normal time rate. Once the gross amount has been calculated, the deductions are worked out, e.g. PAYE, contributions to medical aid, unions and the unemployment insurance fund (UIF), to arrive at the net pay. All of the above are entered in the wages journal/payroll. If wages are to be paid in cash, the clerks in the payroll preparation section will also prepare a "coinage schedule". This schedule is a breakdown of the exact number of notes and coins which are required to make up the paypackets correctly, e.g. if the amount for a particular wage earner is R1 312,20, it should be made up with six x R200 notes, one x R100 note, one x R10 note, a R2 coin and a 20 cent coin.

* a wage clerk will also prepare a cash cheque for the net amount of wages as well as cheques to pay over deductions to the relevant authority.

5.4 Payment preparation and payout

The objective of this function is to transfer the amount owed to employees as per the payroll.

* if wages are paid in cash, what is termed a wage payout is conducted, at which the wage envelopes (packets) are distributed to employees. Payment preparation in a manual system requires that a wage clerk prepare a wage envelope (packet) for each employee, into which the exact amount of cash is placed as per the payroll. (This is the reason that the coinage schedule is produced.) The employees payment advice (which will include details of other forms of "remuneration" such as the company's contribution to the employees pension fund or medical aid) will also be put into the

envelope, and the exterior of the envelope will give details of the employee such as name, employee number, work section. At the payout, the employee must identify himself. He will receive the wage envelope and sign the payroll to acknowledge receipt.

* because of the risk of armed robbery, some companies make use of security firms to obtain the cash from the bank, prepare the wage envelopes and perform the payout.

* a wage payout can give rise to ***unclaimed wages*** : at the conclusion of the payout, there may be unclaimed paypackets for employees who were absent on the day. These should be entered into an unclaimed wage register and safeguarded as they are susceptible to theft. They are normally put under the temporary control of the paymaster who will distribute them as the employees return to work. Unless an employee has given written permission for his or her paypacket to be released to say, another employee or family member, the paypacket should be retained by the company until the employee returns.

5.5 Deductions: payment and recording

* the deductions from an employee's gross pay, such as PAYE, medical aid, etc., do not belong to the company and must be paid over to the respective bodies, e.g. the South African Revenue Services, within the stipulated period. The objective of this function is to ensure that all deductions are actually paid over and that they are paid over within the stipulated time, accompanied by the necessary documents, correctly completed.

6. DOCUMENTS USED IN THE CYCLE

6.1 Employment contracts/employee file

This document formalises the terms and conditions of employment. A copy is kept by the personnel department in the employee's personnel file and/or could be stored electronically.

6.2 Payroll amendment form

This document is used to detail and authorise changes made in the employee register which affect the workforce, e.g. new appointments, dismissals, promotions to higher grades, changes to pay rates. In a computerised system these will be masterfile amendments to the employee masterfile.

6.3 List of employees

This is a list (register) of valid employees and their details, necessary for calculating wages and salaries, provided by personnel. In a computerised system it is called the employee masterfile.

6.4 Clockcard

A card which records the hours which a wage earner has worked. Where hours are automatically downloaded onto the system from the timing device, clockcards are not necessary, but the employee will need to activate the timing device by inserting a swipe card (or similar device) or using a thumb or finger scanner.

6.5 Batch control sheets and batch register

These documents identify batches of clockcards and control their movement between the timekeeping and payroll functions in the cycle. Commonly used in manual systems and in computerised systems where hours must be keyed in from clockcards.

6.6 Deduction tables and returns

These are schedules or returns provided by the entities to which deductions from employees must be paid over e.g. PAYE, medical aid. In a computerised system they will be held electronically on file.

6.7 Payroll (wage journal)

This document (journal) is a spreadsheet which lists employees' names, their work section or cost centre, their overtime and normal hours worked, their gross pay, deductions, and net pay. Applies to both manual and computerised systems.

6.8 Paypackets, payslips, salary advices

The cash due to the wage earner is placed in a paypacket. The payslip or salary advice, notifies the employees of how their remuneration is made up. Where payment is by electronic funds transfer, there will be no paypackets but the employees will still receive a payslip/salary advice.

6.9 Unclaimed wage register

This is the book/journal used to record details of employees who have not collected their paypackets. Does not apply if there is no wage payout.

6.10 Wage (or salary) reconciliation

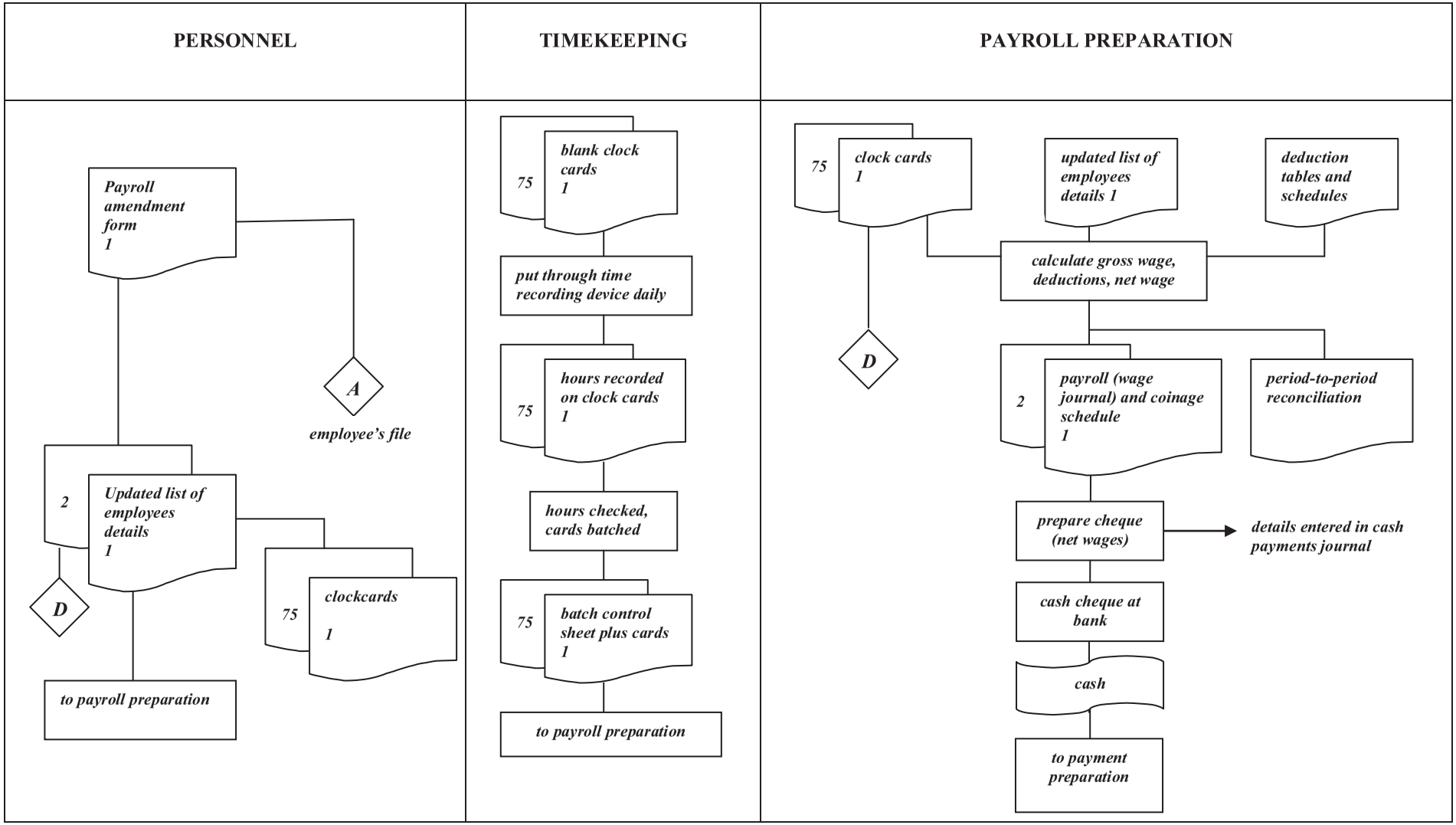
A document which records the reconciliation of the current period's wages to the previous period's wages. (For salaries, it will be done monthly.) Is used in manual and computerised systems.

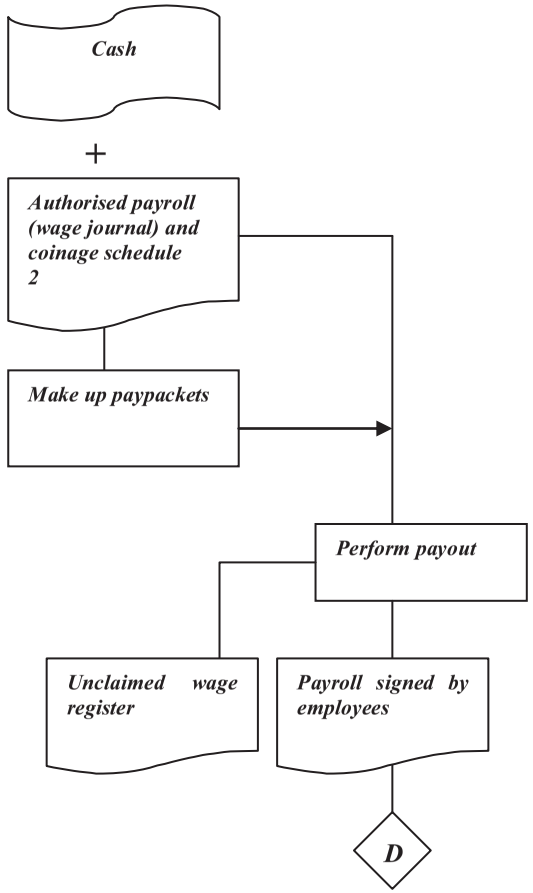
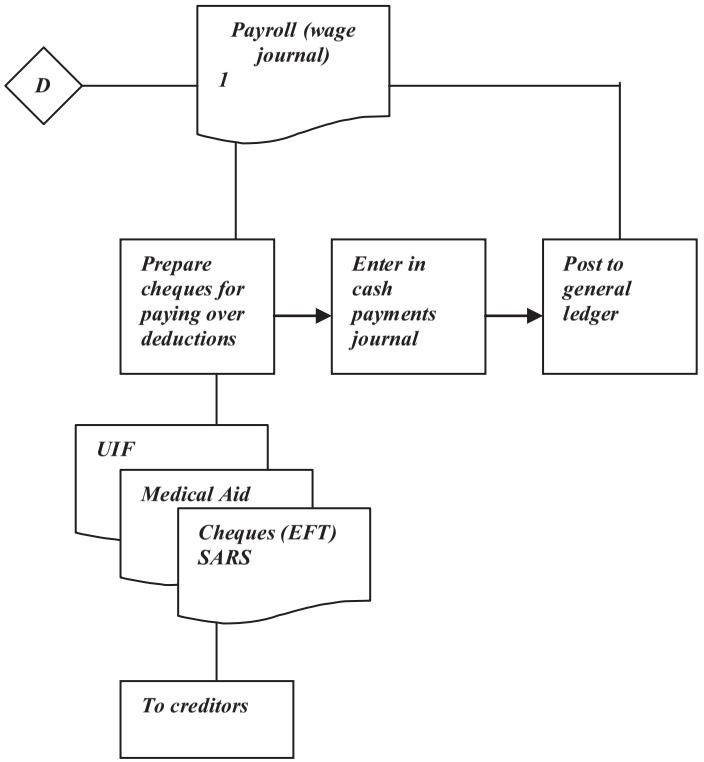
6.11 Logs, variance reports, etc

In a computerised system, the computer can be programmed to compile logs, variance reports, etc. A log is simply a record of an activity that has taken place on the computer, e.g. if a masterfile amendment is made, the computer will automatically "store" the activity, who did it, when it was done, what the amendment was.

7. FLOW CHARTS FOR A MANUAL WAGE SYSTEM

A simple flowchart is provided to give you a "picture" of how a wage system works. If you use the flowchart in conjunction with the narrative description in paragraph 5 above and the schedules on the following two pages, you should obtain a sound basic knowledge.


PERSONNEL
TIMEKEEPING
PAYROLL PREPARATION
Payroll amendment form 1
A
employee's file
2
Updated list of employees details 1
D
75
clockcards 1
to payroll preparation
75
blank clock cards 1
put through time recording device daily
75
hours recorded on clock cards 1
hours checked, cards batched
75
batch control sheet plus cards 1
to payroll preparation
75
clock cards 1
updated list of employees details 1
deduction tables and schedules
calculate gross wage, deductions, net wage
D
2
payroll (wage journal) and coinage schedule 1
period-to-period reconciliation
prepare cheque (net wages)
details entered in cash payments journal
cash cheque at bank
cash
to payment preparation
A = filed alphabetically
= action
= document
D = filed by date
75 = number of clockcards

PAYMENT PREPARATION AND PAYOUT	DEDUCTIONS: PAYMENT AND RECORDING
	

PERSONNEL (HUMAN RESOURCES)		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
To assist with all personnel matters so as to ensure optimum efficiency from the work force, by controlling: * recruitments * dismissals * wage negotiations * labour disputes * staff development To maintain accurate, complete and valid records for all employees and in doing so to provide the information necessary to produce valid clockcards e.g. if an employee is dismissed no clockcard should be available as this increases the risk of creating fictitious employees. Likewise the list of employees' details must be accurate and valid e.g. correct wage rates.	Payroll amendment form (PAF) Employee's file List of employees / employee register	* recruiting/retaining unsatisfactory or unnecessary employees. * incorrect dismissal procedures * unauthorised amendments to employee records • fictitious additions • unauthorised changes in wage rates. * inaccurate or incomplete records

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. All requests for the appointment or dismissal of employees should originate from the section making the request, e.g. factory, stores, administration, etc, and should be in writing and a motivation provided.
2. Requests should be signed by the section head and countersigned by the section manager after reference to the budget. Specifications of the position and the skills required will be agreed by the section and the personnel department.
3. Changes to pay rates, promotions to higher employment grades and any other changes in service conditions, should be decided upon by the personnel department/wage committee after : * due consultation with interested parties, e.g. the union representatives * consideration of relevant laws and regulations, e.g. overtime, pay rates, minimum wage regulations.
4. Such changes should be documented and authorised by the authorising body (e.g. wage committee).
5. ***All*** amendments to employees details arising from 1 to 4 above, should be promptly committed to sequenced payroll amendment forms which should be cross-referenced to the supporting documentation and authorised by a senior member of the personnel section * from time to time the file of PAFs should be reviewed for validity and gaps in sequence.
6. Sound personnel practices should be followed to obtain honest, competent personnel * interviews, background checks, etc.
7. A file should be kept for each employee and should include * copies of relevant PAFs * the employment contract * performance appraisals and disciplinary warnings * personal details including qualifications, background information.
8. Preprinted, properly designed (preferably sequenced) clockcards should be prepared for each employee on the valid employee list. Blank clockcards should be subject to strict stationery controls.

TIMEKEEPING		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
This function is required to keep an accurate and complete record of valid hours worked for which the company must remunerate employees. A system which requires the employee to pass a clockcard through a clocking device to record arrival and departure times is commonly used in manual systems. Daily hours clocked will be calculated and totalled for the period before being sent to payroll preparation.	Clock cards Batch control sheet Batch register	* invalid hours recorded by e.g. • clocking a card for a fictitious employee • employees clocking for absent fellow employees • employees clocking in and leaving the premises * hours on clockcard incorrectly calculated for normal and/or overtime. • normal hours counted as overtime hours (which have a higher rate of pay)

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. Entry and exit points to work area to be: * limited (preferably one) * protected by a "turnstyle" type mechanism * supervised during clocking periods. 2. Clockcards to be prepared by the personnel department, strictly in terms of the authorised employee list, and placed on racks at the entry point. 3. At the end of a wage period, the section administration clerk should collect all clockcards for the period and: * agree number of cards to list of employees in the section * calculate ordinary time * calculate overtime * divide cards into workable batches (e.g. 25) * complete a batch control sheet by : entering batch identification (section and period) details : entering control totals, i.e. record count (number of clockcards), total hours, normal and overtime : signing to acknowledge responsibility. 4. Before the batch of clockcards is transferred to payroll preparation, the section head(s) should * check calculations * authorise overtime (the need to work overtime should be confirmed before it is worked) * check, and sign the batch control sheet. 5. Details of the batch should be entered in a batch register, which will accompany the clockcards to payroll preparation.

PAYROLL PREPARATION		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The role of this function is to calculate gross wages and make deductions from employees which must be subsequently paid over, to arrive at net wages, i.e. create a payroll. The employee's authorised hours must be multiplied by the employee's authorised normal and overtime rates. The appropriate deductions e.g. PAYE, must be extracted from authorised, up to date tables. This is all recorded on the payroll, which is also referred to as the wages journal.	Clock cards Deduction tables Updated list of employees Payroll	* inclusion of fictitious employees * use of incorrect or unauthorised pay rates, hours or deduction tables. * cast and calculation errors.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS

1. On receipt of the batch of wage cards from timekeeping (the section administration clerk), the wage clerk should check details of batches received, e.g. number of batches, number of cards, and sign the register to acknowledge receipt of the batches.

2. The wage clerk should prepare:
   * the payroll
   * a coinage schedule
   * a reconciliation of the difference between the prior periods wages and the current periods wages for the number of employees and amounts for net wages and deductions
     e.g. if the number of employees for period 1 was 250 and for period 2 it was 275, the wage clerk must reconcile the difference of 25. The difference could be 4 dismissals and 29 appointments giving a net change of 25 employees. Obviously there should be authorised payroll amendment forms to support the dismissals and appointments
   * a record of control totals including normal hours and overtime hours per section.

3. A supervisor or second wage clerk should:
   * verify hours and rates used in compiling the payroll against the clockcards and the employee list
   * verify deductions against the relevant tables
   * verify amendments to the payroll against the PAFs and vice versa
   * reperform calculations and the wage reconciliation
   * sign the payroll.

4. The head of payroll preparation should carefully review and sign the payroll and period to period reconciliation, e.g. he may verify a sample of amendments to the authorised PAFs and vice versa.

5. The cheque for wages should be presented with the payroll and period to period reconciliation, to two cheque signatories who should:
   * review the payroll for unusual items, e.g. large amounts, excessive overtime
   * inspect for the presence of control signatures and
   * sign the payroll and reconciliation.

PAYMENT PREPARATION AND PAYOUT		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The purpose of this function is to prepare paypackets containing cash and details of how cash is made up. The paypackets are then distributed at the respective sections (paypoints) to employees. Unclaimed wages must also be recorded.	Payroll Payslips Paypackets Unclaimed wages register	* errors or theft of cash during: • drawing of cash, • making up of paypackets, and • at the payout. * misappropriation of unclaimed wages.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS

1. Wage packets should be made up by two wage department members (physical security over all aspects of cash handling should be extremely tight).

2. On delivery of the payroll and paypackets to a section, the section head should:
   * agree the number of paypackets to the payroll
   * agree control totals e.g. number of cards, total hours, on the payroll to the batch register and
   * sign the payroll to acknowledge receipt.

3. The paypackets and payroll should be locked away until payout.

4. The wage payout should be conducted by at least two employees, e.g. an independent paymaster and the section foreman, both to be present at all times.

5. Employees should:
   * present identification e.g. official staff card, prior to receiving their paypackets
   * acknowledge receipt of their wage packet by signing the payroll
   * count their cash and immediately report any discrepancies to the paymaster. These should be recorded on the payroll.

6. In principle, employees should ***not*** be allowed to accept a paypacket on behalf of another employee.

7. At the conclusion of the payout, the paymaster and foreman who have conducted the payout, should:
   * agree all unclaimed paypackets to the payroll (employees who have not signed)
   * identify clearly on the payroll, all employees for whom there is an unclaimed packet
   * enter the details of unclaimed wages in an unclaimed wage register
   * sign the payroll to acknowledge this control procedure.

8. The unclaimed paypackets and payroll should be retained by the paymaster who should lock them away.

9. When employees wish to collect their unclaimed wages, they must identify themselves to the paymaster and acknowledge receipt of their paypackets by signing the unclaimed wage register.

10. Regular independent reconciliations of unclaimed paypackets on hand and the unclaimed wage register should be performed and the unclaimed wage register reviewed for unusual occurrences, e.g. trend of more unclaimed wages in a section, same employee name appearing frequently.

11. Any wages remaining unclaimed after two weeks, should be banked and a copy of the deposit slip attached to the unclaimed wage register and cross-referenced to the relevant entries.

DEDUCTIONS: PAYMENT AND RECORDING		
FUNCTION	***DOCUMENTS RECORDS***	***RISKS***
The purpose of this function is to record liabilities in respect of deductions from employee remuneration and to pay these over to the relevant authorities timeously. Deductions are made from employees wages on behalf of outside bodies e.g. PAYE is deducted on behalf of the South African Revenue Services and therefore as the deduction is made the liability should be raised and then settled within the stipulated period. Companies will be required to complete a return to accompany the payment.	General ledger Payroll (wage journal) Cash payment journal Return form	* penalties due to non-payment, late payment or underpayment. * criminal/civil charges due to non-payment (this is theft) * incomplete, inaccurate amounts paid over and/or * return forms incorrectly completed.

CONTROL ACTIVITIES INCLUDING BRIEF EXPLANATORY COMMENTS
1. Isolation of responsibility to one employee for raising and paying over deductions. 2. A strict monthly schedule for: * posting the entries to raise the liabilities for the deductions * making the necessary payments on a timeous basis, and conducting * supervisory checks on the above activities should be prepared. 3. The payroll and return forms should be presented to signatories for their scrutiny before the deduction cheques are signed. They should check the return carefully to see that it has been accurately and properly filled in (payments to SARS can be made on their e-filing system). 4. Independent timeous scrutiny of the general ledger accounts for deductions to confirm that they are being promptly cleared, should be carried out by the financial accountant.

8. COMPUTERISATION OF THE PAYROLL CYCLE

Before we deal with the computerisation of this cycle, it will be useful for you to remind yourself of the following points. You can also refer to chapter 8 for a more comprehensive discussion on these points.

8.1 Access.

Many businesses will run their accounting systems on a local area network. Simplistically speaking, this means that there will be a number of terminals, usually from different departments, "linked" together and sharing resources. So access to the network and to individual applications, must be carefully controlled;

* access to the network should only be possible through authorised terminals
* only employees who work in the various functions of the cycle need access to the payroll application and only to those modules or functions of the application necessary for them to do their jobs (least privilege/need to know basis). Certain managers will have extensive read access for supervisory and review purposes.

Various techniques are used to control access. For example, the user

* must ***identify*** himself to the system with a valid user ID
* must ***authenticate*** himself to the system with a valid password
* will only be given access to those programmes and data files to which he is ***authorised*** to have access in terms of his user profile.

Once the user has got onto the system, access is usually controlled by what appears or does not appear on the user's screen. For example, only the modules of the application to which the user has access will appear on the screen, or alternatively, all the modules will be listed, but the ones the user has access to will be highlighted in some way, e.g. a different colour. If the user selects a module to which he does not have access (this is determined by his user profile), nothing will happen and/or a message will appear on the screen which says something like "access denied". In another similar method of controlling access, the screen will not give the user the option to carry out a particular action. For example, a schedule of overtime hours may be on a file awaiting approval by the production manager. Although other users, e.g. a cost centre foreman, may have access to this file for information purposes, when they access the file their screens will either not show an "approve option", or the "approve option" will be shaded and will not react if the user "clicks" on it. Only the production manager's screen will have an approve option which can be activated.

8.2 Menus.

Current software is all menu driven and generally easy to use. Menus can be tailored to the specific needs of a user (based on the user profile) and "items" can be selected by a simple "click of the mouse". Menus facilitate access control and segregation of duties.

8.3 Integration.

The extent to which the accounting system is integrated will vary, but most systems these days are integrated in the sense that a transaction entered onto the system, will instantly update all the records it affects. For example, the processing of a salary will simultaneously update the salaries account, deduction accounts and the salary employee masterfile. This significantly improves the accuracy of the records ***but*** makes the control over input extremely important.

8.4 Screen aids and programme (automated) checks.

These control techniques which are obviously only available in computerized systems, help ensure that transactions processed actually occurred, were authorised and are accurately and completely recorded and processed. The extent to which these are incorporated will vary depending on the quality and cost of the software. These controls are essentially preventive at the input stage and detective thereafter.

8.5 Logs and reports.

A computer can be programmed to produce any number of logs and reports. These can be used as detective controls or for monitoring performance. For example, in the payroll cycle, a log of all employee masterfile amendments should be produced by the computer. This log will be a listing of all amendments that were made, what the amendment was (e.g. addition of a new employee), who made the

amendment and when it was made. "Read only" access to this file will be given to a senior member of the human resources/accounting section so that the amendments made can be confirmed as being authorised, accurate and complete by reference to the masterfile amendment forms. This log can be printed out or accessed on screen. Another example in a payroll system would be the production of a report of all overtime worked per cost centre per week for say, the last six weeks which can be used to monitor the performance of the production personnel. The important point about logs and reports is that unless an employee actually uses them and follows up on any problems, they are worthless. Their huge potential value is that if the log and report files are properly access protected, they provide ***independent*** evidence of what has taken place on the computer. They form a very important part of the ***audit trail***.

8.6 ***Matching and minimum entry***.

Once data is in the database other data can be "matched" against it. A simple example would be where an employee's number is matched against the employees' masterfile to determine whether it is a valid number. The fact that data is stored in the database also means that the principle of minimum entry can apply. For example, if the payroll clerk wishes to call up an employee's earnings record, there is no need to enter anything other than the employee number. No further information needs to be keyed in. The speed, accuracy and completeness of input is enhanced.

8.7 ***On system approval.***

Where hardcopy documents require approval, it is usually just a matter of presenting the authorising employee with the document and supporting evidence. In a computerised system, approval is frequently given on the system itself and the supporting evidence is also frequently on the system as well. There will be variations on how this is done, depending on the software. In a payroll system the foreman may approve a file of overtime hours worked, on the system.

8.8 ***Audit trail.***

An audit trail is a record of the activities which have happened on the system which enables the sequence of events for a transaction to be tracked and examined, from start to finish. It should be possible to identify a wage expense reflected in the general ledger and trace it back to the hours worked by the individual employees whose wages make up the payment selected. A system where there is a poor audit trail, will be a weak system. The trail will often be a combination of electronic and hardcopy data.

A NARRATIVE DESCRIPTION OF A COMPUTERISED (WAGE) PAYROLL SYSTEM BY FUNCTION

A company's wage payroll system will be a combination of manual and computerised functions and various combinations are possible. For example, a conventional clock card system could be used for timekeeping, with employees hours being captured (keyed) into the system for processing, and payment could be conducted at a weekly wage payout or amounts could be transferred electronically into employees' bank accounts. Alternatively, more sophisticated computerised timing devices could be used to record employee hours worked. This information would then be downloaded for processing and the production of the payroll. Payment could be carried out at a wage payout but it is more likely that payment would be by electronic funds transfer. For the purposes of this illustration, we have decided to discuss the wage payroll system for a company which uses a biometric scanning device (which will be explained later) to control access, record hours worked and download them for processing, and in which employees are paid by EFT.

Most companies will make use of packaged payroll software which has been developed to meet the needs of the company, the employee and SARS. The software will generate information required by SARS, e.g. employee earnings, PAYE, etc. and will often interface with the SARS efiling system. It will also be compatible with the company's banking "system" to facilitate EFT payments. We have assumed that the company is large enough to have sound segregation of duties.

The employee masterfile

The employee masterfile is central to the payroll system. The company will have an hourly paid employees masterfile and a salaried employees masterfile; we are dealing with hourly paid (wage) employees. Integrity of the masterfile must be maintained and access to the masterfile, particularly write access, i.e. the ability to make amendments, must be strictly controlled. Equally important is the control over the amendments themselves to ensure they are authorized (valid), accurate and complete. Amendments to the employee masterfile include adding a new employee, changing a pay rate or changing an employee's banking details.

Much of the information on the employees masterfile is the responsibility of the human resources section, so it makes sense for this section to be primarily responsible for the integrity of the file and the amendments. Other companies may have a separate department which deals with all matters relating to the payroll but however it is set up, control over the masterfile remains very important. If all amendments are subject to strict controls, the risk of fraud is considerably reduced. All amendments should be logged and there must be independent reconciliation and review of the log by a senior employee, e.g. the financial director.

Activity/procedure	***Control, comment and explanation***
1. Record all masterfile amendments on a source document.	1.1 ***All*** amendments to be recorded on hardcopy masterfile amendment forms MAFs (no verbal instructions) (see Note (b) on page 13/18).

	1.2 MAFs to be pre-printed, sequenced and designed in terms of sound document design principles.
2. Authorise MAF.	2.1 The MAFs should be * signed by two senior employees (e.g. human resource manager and the head of the section in which the employee works) after they have agreed the details of the amendment to the supporting documentation, e.g. the letter of appointment for a new employee * cross referenced to the supporting documentation.
3. Enter only authorised masterfile amendments onto the system accurately and completely.	3.1 Restrict write access to the employee masterfile to a specific member of the personnel section by the use of user ID and passwords (see Note (a) on page 13/18). 3.2 All masterfile amendments should be automatically logged by the computer on ***sequenced*** logs and there should be ***no write access*** to the logs (sequencing allows subsequent checking of the MAFs entered for authority). 3.3 To enhance the accuracy and completeness of the keying in of masterfile amendments and to ***detect invalid conditions***, screen aids and programme checks can be implemented. 3.4 On screen check of details entered against the MAF by a second employee. ***screen aids and related features*** * minimum keying in of information. For example when amending existing employee records, the user will only key in the employee number to bring up all the details of the employee * drop down list for allocating an employee to a cost centre, department or section * screen formatting, screen dialogue * the employee number for a new employee is generated by the system. ***programme checks***, e.g. (see Note (c) on page 13/18) * adding a new employee • mandatory fields, e.g. employee identity number (passport number) and income tax number, and full banking details. New employees who have not registered with SARS are required to do so and will be assisted by the personnel department

	• dependency check, e.g. acceptance of the entry of the hourly wage rate may depend on the grade or level which has been entered for the new employee • range and/or limit checks on the wage rate field • field size check, e.g. identity number has 13 digits • alphanumeric check on wage rate field * changing the data of an existing employee • no write access to identify number field, income tax number etc • verification (matching) of employee number (incorrect number, no amendment) • minimum entry, e.g. employee number brings up all the necessary data relating to the employee.
4. Review masterfile amendments to ensure they occurred, were authorised and were accurately and completely processed.	4.1 The logs should be reviewed regularly by a senior staff member e.g. financial director. 4.2 The sequence of the logs themselves should be checked (for any missing logs). 4.3 Each logged amendment should be checked to confirm that it is supported by a properly authorised MAF and 4.4 That the details, e.g. identity numbers, banking details, are correct. 4.5 The MAFs themselves should be sequence checked against the log to confirm that all MAFs were entered.

Note (a): The authority needed to enter different types of masterfile amendment can be given (by the user profile) to different levels of employee e.g. changing an employee's banking details may be restricted to a single senior employee, but changing an address or contact details could be assigned to a lower level employee.

Note (b): Unused MAFs and other important supporting documentation should be subject to stationery controls as it is more difficult to create an invalid masterfile amendment without the source document.

Note (c): A masterfile amendment should be carefully checked in all respects before it is authorised. In respect of, for example, the addition of a new employee, before an offer of employment is made, the personnel department should verify important details with independent evidence, e.g. the identity number against the individual employee's ID book, the income tax number and banking details, against official documents from SARS and the bank respectively. There should be a minimum of errors or invalid conditions having to be identified (detected) by the programme controls. Each company will decide for itself the extent of programme controls they wish to implement.

"Timekeeping" linked to the computerized payroll system
Where the timing device which records the entry and exit times of employees, automatically transfers the hours worked to the payroll preparation section for the preparation of the payroll, there is obviously no need for clockcards, batch controls, the physical transfer of the batches or the conversion of the source data (hours) into machine readable form. * In a computerised clocking system, the employee is required to "swipe" his identification tag (or similar) through an electronic timing device. The timing device "reads" the information stored on the magnetic strip on the identification tag and records the time of entry or exit in a file against the employee's name "taken" from the magnetic strip. * When the payroll is processed, the file of hours worked is imported and the wage application software automatically calculates the hours worked by the employee for the wage period. (No clockcards used.) * One of the weaknesses of this system (as with the clockcard system), is that an employee could "swipe" the identification card of another employee who has not actually come to work, thus creating "fictitious" hours worked. This problem can be overcome by employees having to activate the timing device by presenting biometric data. The most common of these is the thumb or fingerprint. So to have his time of exit or entry recorded, the (valid) employee must activate the timing device. With this system, when an employee is engaged, his fingerprints will be taken and stored on the computer. When the employee places his thumb or finger on the scanner (timing device) at the entry/exit point to the workplace, recording of the time of entry or exit will only be recorded if there is a match of the print to that employee's print stored on the computer. Again with this system, the hours worked will be automatically calculated and imported (downloaded) for processing. For the purposes of this illustration, assume that the company uses a biometric reader for the identification of employees and recording hours worked.

Activity/procedure	*Control, comment and explanation*
1. Storing biometric data on the system.	1. For identification of employees to be controlled by biometric data, a thumb print/finger print will need to be stored on the system so that when the employee places his thumb on the scanner, it has a set of prints against which to "match" the thumb print * the biometric data will be stored on the employee masterfile * access to the module which facilitates the recording of the data should be strictly controlled (conventional logical access controls) * the responsibility for capturing the biometric data should be assigned to the personnel department

	* programme controls will prevent the biometric data from being replaced (a variation of write access to the field).
2. Employee identification and recording of hours worked.	2.1 The basic controls around exit/entry should apply * limited entry points * physical access controls, e.g. successful scanning of the employee's thumb print activates a turnstile mechanism * entry/exit point should be generally observed by security.
3. Reviewing employee attendance	3.1 Supervisory personnel should make use of the timing device's storage capabilities to access information pertaining to employee attendance on the system, e.g. absent employees, late arrivals, unexplained exits from the work place, etc. These reports can be generated daily, weekly and in various formats (may also be available in real time).

Payroll preparation
At the end of the wage period, the payroll must be prepared. The hours which have been worked, both normal and overtime for each employee, will be on the system waiting to be processed against the employee's hourly wage rate to arrive at the gross amount to be paid. Before processing takes place, the hours worked, particularly overtime, should be scrutinized and approved by supervisory staff. Weekly deductions from the gross amount will also be processed, e.g. PAYE, UIF, medical aid. However, there may also be other amounts due to an employee which are not based directly on the hours worked, e.g. incentives/bonuses, which must be entered onto the system. There may also be other deductions e.g. a garnishee order (a court order which requires an employer to deduct an amount from an employee's wages to repay a debt), or a loan repayment which must be entered.

Activity/procedure	*Control, comment and explanation*
1. Approval of hours worked.	1.1 Before payroll preparation commences, a schedule of normal and overtime hours for the week should be printed out and sent to the foreman (or other supervisory staff) for approval. 1.2 The foreman should * check the schedule for any incorrect or unusual hours recorded, e.g. • normal hours in excess of 40 hours per week • high overtime hours and low normal hours * confirm that the overtime hours recorded were authorised prior to being worked and/or that they were actually worked (note the recording of hours worked will be very accurate, but the timing device does not "know" if the hours recorded as overtime, were authorised) * confirm that there are hours worked for all employees and that any missing normal hours agree with the attendance reports generated by the access/scanning device. 1.3 Any alterations to the schedule should be recorded on the schedule with reasons and signed by the foreman. Any changes, e.g. any increases or decreases in overtime hours which the foreman requires, should be counter-signed by another supervisory level employee, Note: the approval of the hours worked schedule could take place on the system and the usual controls relating to on-system approval would be in place, e.g. access to the hours worked file restricted, no write access for the foreman, alterations referred back to the payroll department. Any alterations made by the payroll clerk would be logged for subsequent review.
2. Entering additional earnings and deductions	2.1 The payroll clerk responsible for preparing the payroll will be responsible for entering these on the employee's record. * access to the applicable module (payroll preparation) will be restricted in the usual manner, i.e. user ID, password, user profile * to access a particular employee's record, a valid employee number will have to be entered (verification check) * it is usually unnecessary for the payroll clerk to have to enter each

	employee's number; the software will start with the first employee and automatically bring up the next employee's record as each record is confirmed. 2.2 On accessing the module, the screen will come up formatted as an employee payment record. This will reveal * all standing data applicable to the employee, e.g. name, cost centre, grade, hourly rates etc * fields containing year to date earnings including pension fund and medical aid contributions, deductions, net pay etc * fields revealing the current period's normal and overtime hours worked, the company's contribution to a pension fund or medical aid, etc * a selection of fields designated in terms of additional categories of amounts to be paid to the employee, e.g. travel claims, incentive bonuses, or deductions to be made, e.g. garnishee orders. 2.3 There will be no write access to * the standing data fields * year to date fields * some of the fields already "populated" by the payroll software such as medical aid contributions and deductions, contributions to pension funds. 2.4 If hours worked have already been approved on the system, there will also be no write access to the current period's hours worked fields. 2.5 If these fields need to be altered in terms of the hardcopy hours worked schedule * there may be limit checks on the normal and overtime fields * all changes will be logged and reviewed before the payroll is finally approved. 2.6 Additional amounts to be paid to an employee should be authorised in writing by appropriate personnel, e.g. an incentive bonus should be approved by the employee's section head and say, the financial director, after confirming compliance with the underlying conditions for paying the bonus and reperformance of the bonus calculation has taken place. The same requirements should apply to any additional deductions entered * screen prompts may alert the payroll clerk to the fact that a particular deduction must be made for a specific employee. 2.7 As the objective is to ensure that the source data is absolutely correct before processing takes place, a second payroll clerk may check the employee payment records in detail or selectively. (The second payroll clerk would not have write access).

3. Processing to create the payroll	3.1 Actual processing will be carried out by the computer without human intervention. The computer will only process the data it is supplied but will do it accurately and completely. 3.2 Processing will not commence until the employee payment records have been "confirmed" (after all the controls described above have been carried out) by the payroll clerk. Even though the "input" has been subjected to stringent controls, additional programming controls may also be implemented to detect invalid conditions e.g. * reasonableness/limit checks; the net wage for an employee may be unreasonable when compared to the employee's employment level, e.g. a wage of R10 000 may be unreasonable for an unskilled worker or a net wage exceeding R15 000 may be an invalid condition * matching; the computer may match the number of payment records it has processed against the employee masterfile and produce a report of any missing records (control total principle) * cross-cast tests; totals in the net wages column must equal totals in the gross wages column, less totals in the deductions columns, for each employee and the payroll as a whole * run to run totals; the total of the year to date of net earnings for all employees in the employee masterfile at say, the end of period 14, will be computed. The total of all net earnings for all employees for period 14 will then be computed, added to the total of year to date net earnings at the end of period 13 and compared to the same total of net earnings at the end of period 14, as initially computed.
4. Approval of the payroll	4.1 Once processing is complete, the payroll and a number of supporting schedules will be produced for final checking by the payroll administrator. He will carry out checking procedures such as * agreeing the number of employees on the payroll to the number of employees on the employee masterfile * following up on the run to run balancing reports * following up on any exception reports, e.g. a net earnings amount identified as not reasonable by programme checks * reviewing analytical summaries which may have been produced, e.g. comparison of wages between cost centres, sections and corresponding prior periods

	* reviewing overtime schedules * reviewing the period to period reconciliation and agreeing it to supporting documentation. For example, changes in the employee headcount should be checked against the log of masterfile amendments and where necessary, to engagement or dismissal documentation. 4.2 If any errors are detected, they should be followed up * the payroll administrator should not have write access to the file, and * changes should be referred back to the wage clerk for correction * all changes should be logged. Note : the review process can be on screen or on hardcopy documents and additional senior supervisory/management, e.g. section heads, production manager, etc may be introduced into the review process. 4.3 Once the payroll administrator is satisfied with the payroll file, he will select the approve option and there will be no further write access to the file, and for confidentiality purposes, read access should be given to only those who need it. (This is in essence, an output control.)

Payment to employees by electronic funds transfer

The final step is to transfer the correct amount owed to each employee. As discussed in chapter 9, electronic funds transfer is a very fast and efficient method of making payments, but it is perhaps for these very reasons that the risk of fraudulent payments (theft of funds from the company's bank account) will be very high if strict controls are not in place. The controls over EFT payments will centre around

* controlling access to the employee masterfile. It should not be possible to add a fictitious employee to whom fictitious payments can be made, and it should not be possible to alter an existing employee's banking details other than under strictly controlled conditions
* approving details and amounts to be paid to the employee
* controlling access to the company's bank account
* a review of EFT payments actually made.

The preceding charts have dealt with controlling the masterfile and preparing the payroll, so all that remains is to deal with the two remaining aspects of control.

We have assumed, for the purposes of this illustration, that wage earners are paid every two weeks, not that this unduly affects the controls over EFT payments.

Activity/procedure	*Control, comment and explanation*
1. Access to the bank account on the internet	1.1 The bank's EFT software will be loaded onto a limited number of the company's terminals. 1.2 Access to the bank's site on the web will be gained in the normal manner but once the employee gets onto the site, an additional PIN number supplied by the bank and a password unique to the employee, will have to be entered to gain access to the company's account. • the privilege to access the company's account will only be granted to employees who need access to the bank account to carry out their duties. 1.3 If this identification and authentication process is accepted, a menu of the functions available to the company will appear on the screen, e.g. balance enquiry, payment query, download bank statement, make EFT payment. 1.4 Access to these functions will be directly linked to the employee's user profile on a need to know basis. The function which needs to be most protected will be the ability to make an EFT payment • this privilege will be granted to a limited number of senior personnel (much like giving senior employees cheque signing powers) • an additional ***authentication*** procedure will be required, e.g. an additional one time password or the insertion of a physical device into the USB port of a terminal on which the bank's software is loaded (see chapter 9/19 for a discussion on these devices).
2. Approving (effecting) the payment We will assume for the purposes of this illustration, that the company's bank requires a small device such as a "dongle" to be inserted into the USB port of a terminal on which the bank's software is loaded. We will also assume that the payroll administrator, the financial manager and the head of the personnel section have the privilege to effect an EFT payment.	2.1 At least two of the three authorized employees will be required to effect the payment of wages, e.g. the payroll administrator will authorize the payment and the head of personnel will release it. 2.2 Once the payroll administrator is satisfied with the payroll he will select the "first confirmation" option and a system generated message will be sent to the head of personnel informing him that the payroll file is awaiting his approval. 2.3 The head of personnel will then access the file of payments and carry out whatever procedures he deems necessary to be in a position to authorize the payments, e.g. review of reasonableness, access of masterfile amendment logs, reference to original documentation. * the second "signatory" (the head of personnel) will ***not*** have ***write*** access to the file so cannot for example, add an additional fictitious employee to be

	paid * once the "second signatory" is satisfied, he will click on "second confirmation". * the "second confirmation" cannot be activated before the "first confirmation". 2.4 The file of payments will now be fully approved, and the clicking on the second confirmation will automatically convert the file to a format compatible with the bank's EFT software, the only data that the bank requires is the employee code, bank name, employee surname and account details. 2.5 Once this has been done, the payroll administrator will click on the ***authorize*** option (the dongle will be inserted into the USB port) and the head of personnel will click on the ***release*** option. * the ***release*** activity cannot be activated before the ***authorize*** option. 2.6 Additional controls which should be implemented are * automatic shutdown after three unsuccessful attempts to access the company's bank account on the system * logging of attempts at unauthorized access (successful attempts will also be automatically logged) * the number of bank accounts to which transfers from the ***main*** bank account can take place should be limited to protect the main bank account. For the payment of wages, an amount equal to the total of individual payments to employees should be transferred to a separate account and the actual transfer to employees' bank accounts should be made from this separate account. Transfers to employees' bank accounts could be scheduled only to take place on specified dates (every two weeks) * a limit on the total amount which can be transferred within a 24 hour period as well as a limit on individual payments can be arranged with the bank * data should be encrypted * conventional password controls will apply and physical authentication devices, in this case the dongle, must be kept safe and secure at all times. 2.7 The electronic funds transfer will update the employees masterfile, cash payments journal and deduction accounts. Note: Amounts paid to SARS, e.g. PAYE, UIF and the skills development levy will be paid over to SARS using the e-filing system. The company will register with SARS and submit the necessary information online. Security on payments made by e-filing is enhanced by the fact that transfers can only be made to the SARS bank account. It would be impossible for an employee to make a

	fraudulent transfer to his own bank account through the e-filing system. Amounts payable to other entities, e.g. medical aid, pension funds, etc will be paid by EFT in the conventional manner and subjected to the same strict controls.
3. Detection of unauthorized payments	3.1 Within a day or two of making the electronic funds transfer (EFT), the accountant (or similar level employee) should download a copy of the bank statement for the wages account and compare it to the schedule of payments to employees. Payments to medical aid, pension funds etc, would be checked promptly against a downloaded statement of the applicable bank account.

Processing controls
As mentioned in chapter 8, the accuracy, completeness etc, of processing, are evidenced by reconciliation of output with input and the detailed checking and review of output by users, on the basis that if input and output can be reconciled and checks and reviews reveal no errors, processing was carried out accurately and completely and only transactions which actually occurred and were authorised, were processed. To make sure it does its job, the computer will perform some internal processing controls on itself, e.g. arithmetic accuracy tests, but the user will not even be aware that these are going on. The users within the cycle make use of the logs and reports which are produced relating to their functions, whilst the IT systems personnel make sure that processing aspects of the system are operating properly.

Summary	
The description of the system described above, provides an illustration of how the control activities described in chapter 5 (and referred to in ISA 315 (Revised)), can be implemented. It also provides an illustration of how specific automated (programme) controls can be introduced. For example:	
Segregation of duties	* Separation of functions, e.g. timekeeping, payment preparation, payment. * Separation of responsibilities within functions, e.g. authorising overtime, entering payment record amendments, checking the period to period reconciliation.
Isolation of responsibilities	* Isolating responsibilities through granting access privileges, e.g. only head of personnel can release an EFT payment. * The foreman signs the schedule of hours worked.

Approval and authorisation	* A masterfile amendment to add an employee to the employee masterfile is approved by the head of personnel. * The payroll administrator approves the payroll.
Custody	* Access to the bank account (custody of the company's money) is strictly controlled by user IDs, PINs and passwords (those with authority to make an EFT are effectively the custodians of the company's cash).
Access controls	* All users on the system must identify and authenticate themselves by IDs and passwords and what they are authorised to do is reflected in their user profiles. * Additional access controls such as terminal shut down and logging of access violations are in place.
Comparison and reconciliation	* The system matches the payment records it has processed against the employee masterfile to identify any employees for which no record has been produced. * The system reconciles the total net earnings for period two with the total net earnings for period one.
Performance review	* Comparison of overtime worked period to period and section to section. * Monitoring complaints from employees pertaining to errors in overtime payments, deductions or incentive bonuses.
Control techniques and application controls	* Screen aids and related features • minimum entry : keying in the employee number when preparing the period payment record brings up all the detail pertaining to an employee • screen formatting : employee payment record, payroll • mandatory fields : new employee's ID or passport number. * Programme checks • validation check on employee number • limit checks/reasonableness checks on net earnings for an individual • dependency check: pay rate dependent on grade of employee. * Output control • restricted distribution of the payroll, both physically (minimum printed copies) and on the system (logical access control) • bank statement (audit trail) checked against EFT payments entered onto the system.
Logs and reports	* Log of changes to existing employee's banking details, hourly wage rates * Analysis of wages paid by cost centre.

This does not cover every control, policy or procedure that could be in place and is not intended to. This knowledge will only be acquired when you go into different companies and work with their systems.

9. SALARY SYSTEMS: MANUAL AND COMPUTERISED

It is not necessary to describe separately a salary system as the risks and control procedures are essentially the same as for a wage system. The obvious difference is that salary systems do not have a timekeeping function; a salary is a set monthly amount regardless of the hours worked by the employee. Salaried employees may still have to swipe their identification card or have their thumbprint scanned on arrival at work, but this is simply a security check. The other functions within a payroll system will still be required, i.e.

9.1 Personnel (human resources)

Personnel (human resources) will play the same role of recruiting, resolving issues, training, etc and maintaining records of the salaried staff including the maintenance of the employee masterfile in a computerized system. Changes such as adding an employee or changing the amount of a salary must still be strictly controlled whether the system is manual or computerized, e.g. masterfile amendments must still be authorized, correctly entered, logged and independently reviewed.

9.2 Payroll preparation

The objective of this function is to produce a salary payroll which shows the gross amount, deductions and net amount payable to each employee. The necessary supporting documentation e.g. payslips, month-to-month reconciliation, will also be produced.

9.3 Payout preparation and payment

In a manual system, salaries will be paid by cheque and the normal control procedures over cheque payments will be in place. Where payment of salaries is by electronic funds transfer, which is very common, the full range of controls over EFTs should be in place.

9.4 Deductions: payment and recording

This is no different from the pay over of deductions in a wage system. Payment can be by cheque or EFT (including e-filing) and the full range of controls should be in place.

10. THE ROLE OF THE OTHER COMPONENTS OF INTERNAL CONTROL IN THE PAYROLL SYSTEM

This chapter has concentrated on the accounting system which is part of the ***information system*** and ***control activities*** components of internal control. However, these components are affected by the other components of internal control, so a brief mention of the role of the other components is necessary.

10.1 The control environment

The control environment within the cycle will be directly influenced by the control consciousness of the company as a whole. With regard to the cycle specifically, the tone will be set by the manner in which the personnel department conducts itself with regard to its labour practices, such as recruitment, health and safety, settling of labour disputes, negotiations with employee unions etc, and proper training. Employees should be fairly remunerated and be paid the correct amounts due on time. This type of environment is likely to reduce the incidence of absenteeism, a poor attitude to timekeeping and attempts at claiming invalid overtime. Senior employees responsible for approving masterfile amendments, the payroll and EFT payments, should be diligent and be seen to be diligent. For example, supporting evidence for masterfile amendments should be scrutinized before approval is given, random number generator devices or "dongles" and passwords should not be given to other employees to authorise or release payments. This diligent attitude will dissuade employees from colluding to add fictitious employees.

As we pointed out earlier, the payroll cycle provides a legitimate process for getting money out of the company, so if controls are not strictly enforced, theft and fraud will surely follow.

10.2 Risk assessment process

The company's formal risk assessment process will address the risks which may have a direct affect on the cycle, e.g. labour strikes, a lack of skilled personnel, HIV/AIDS, and information technology risk (EFT). Less formal risk assessment can occur within the cycle itself with the employees in the section evaluating the risks and responses already in place to address the specific risks facing the section, e.g.

failure to comply with the (quite extensive) labour laws, recruiting the right personnel, avoiding strikes and work stoppages, late or inaccurate processing of amounts owed to employees.

In a smaller entity, the risks of contravening the labour laws can be a major risk. Due to a lack of resources, formal employment practices may give way to informal practices such as employing unregistered/illegal workers, paying sub-minimum wages and failing to comply with health and safety regulations.

10.3 Monitoring

This is the ongoing monitoring of the cycle to determine how the cycle is doing over time. Broadly stated, the objectives of the cycle would be to comply with the labour laws, remunerate fairly whilst remaining within budgeted costs, minimise fraud, and generally maintain a reasonably content workforce. These can be monitored by period-based comparisons of such matters as

* hours lost to strikes and downtime
* the number of disciplinary hearings
* employee turnover, shortages of particular skills
* incidences of fraud.

Monitoring can be conducted by the board through scrutiny of reports on the above matters provided by section heads or an internal audit team.

THE PAYROLL AND PERSONNEL CYCLE AT PRORIDE (PTY) LTD

1. INTRODUCTION

The staff compliment at ProRide (Pty) Ltd is approximately 60 employees. This means that the cycle is relatively easy to control, but internal control in the cycle is still taken very seriously.

2. CATEGORIES OF STAFF

2.1 Permanent salaried staff

All administration staff fall into this category as well as the warehouse manager and warehouse foreman.

2.2 Hourly paid staff

All other staff such as pickers and dispatch clerks, etc, are hourly paid. In prior years the company made use of a labour broking company to supply and administer its hourly paid staff. However, for various reasons ProRide (Pty) Ltd no longer uses a labour broker and administers the wage payroll itself. This has resulted in the appointment of an additional administrative assistant who in addition to other duties, administers the wage employee payroll, and reports to the financial manager. The company also makes use of a legal consultant to ensure that all legal requirements are satisfied.

HOW THE SYSTEM WORKS (hourly paid staff)

1. Hiring and Dismissal

If an additional hourly paid worker is required, a written motivation must be prepared by Reg Gaard (warehouse manager). The motivation must be specific as to the role the new employee will play and the skills required e.g. must be able to operate a forklift. This motivation is sent to Brandon Nel (financial director) for authorisation. Before authorising it, Brandon will refer to the financial budget and consider the foundation of Reg Gaard's motivation.

If the financial director is satisfied with the motivation, Reg Gaard, the warehouse manager, will approach the municipal employment agency which keeps a register of skilled and semi-skilled workers. For every position at ProRide (Pty) Ltd, three individuals will be interviewed by Reg Gaard and the payroll administrator. Background checks are carried out and where possible information on on-line databases sought, e.g. whether the individual has a criminal record.

Any individual who is employed must be registered with SARS (have an income tax number) (ProRide (Pty) Ltd will assist with registering the individual) and must have a bank account (again ProRide (Pty) Ltd will assist if the individual does not have a bank account) as wages are all paid by electronic funds transfer.

Where an employee is to be dismissed, e.g. for theft, a full disciplinary procedure is conducted under the guidance of the company's legal consultant.

Once an appointment or dismissal procedure has been completed, the documentation is signed off by the warehouse manager and the financial director and a masterfile amendment form is completed. All masterfile amendments are logged by the computer and the log subsequently checked by the financial manager to the supporting documentation, e.g. employee details, banking details, tax numbers are carefully checked to source.

2. Rates of Pay and Rate Changes

Hourly paid employees are graded in terms of their job description e.g. picker, forklift driver, despatch clerk, and each grade has a range of hourly pay rates. Rates of pay are increased annually. A process of negotiation between employee representatives, the company's legal consultant, the warehouse manager, and the financial director takes place to determine the annual percentage increase for hourly paid staff.

Documentation arising from these discussions is used as a basis for preparing a masterfile amendment to adjust the individual employee's records in the wage employee masterfile. The MAF is signed by the financial director and the warehouse manager and amendments are logged by the computer as normal, for subsequent checking by the financial manager.

3. Timekeeping

ProRide (Pty) Ltd has invested in a biometric reader/access control system to control access to the warehouse and to record hours worked (normal and overtime), for all hourly paid staff. The "clocking" procedure is not supervised but the entry/exit point is visible from the warehouse foreman's office

* to record their times of arrival and departure and gain access, employees must place their thumb on a scanner. The access device compares the scanned print to the prints held in the employee masterfile and if there is a match (which is normal)
  - the employee will be granted access through a turnstile mechanism and
  - the time of arrival (or departure) will be stored against that employee on the system

* the access device automatically calculates and stores the normal and overtime hours worked each day

* at any time of the day the warehouse manager (Reg Gaard) and the financial manager (Johan Els) can access various reports on the system relating to the clocking process, e.g. a report on absentee workers, employees who have arrived late or left early the previous day, and overtime worked (if any) for the previous day. These reports can be reviewed on screen or printed out

* at the end of each week (note: wages are paid every two weeks) a schedule of hours worked for each employee, split between normal and overtime, is printed out, carefully checked by Reg Gaard and authorised. Any changes are recorded.

4. Payroll Preparation

ProRide (Pty) Ltd makes use of reputable packaged payroll software which is menu driven and relatively easy to use. The software is loaded on the payroll administrator's PC and conventional access controls apply. Access to most functions is restricted to the payroll administrator. Wages are paid every two weeks

* to prepare the payroll for the period, the payroll administrator accesses the software and a menu of various functions appears on the screen
  - if for example, a new employee is to be added, the administrator will select the "update masterfile" option. This will reveal a sub-menu of options and the administrator will select the "add employee" option. (This option is restricted to him through his user profile)
  - at this point the screen will come up formatted as a blank employee record and the administrator will enter the new employee's details. Important mandatory fields are the employee's identity number, income tax reference number and banking details. There are also other common programme controls to enhance the accuracy and completeness of entry, e.g. hourly wage rate is dependent on employee grade

* once any new employees have been added, the payroll administrator will select the "prepare payroll" option. This will bring up the payment record for the first employee on the masterfile. The record will reflect
  - the employee's details
  - earnings, deductions etc for the year to date
  - the hours worked for the two week period (normal and overtime)
  - a number of designated blank fields into which the administrator can add data, e.g. a deduction for a loan repayment

* before proceeding to the next employee's payment record, the administrator will
  - confirm the hours worked (both normal and overtime) against the hours worked schedule signed by the warehouse manager and make any alterations required
  - enter any other adjustments to be made, e.g. special bonus or loan repayments

* when the administrator selects the "confirm" option, the computer will process the changes to complete the payment record for the period

* all adjustments are logged by the computer for subsequent checking by the financial manager

* once all employees payment records have been reviewed and updated, the system produces the payroll for the period. The system also produces a period to period reconciliation and various other analytical reports can be generated, e.g. wages for the period by cost centre, employee grades etc, but these are not required by ProRide (Pty) Ltd

* at this point Johan Els the financial manager, will access the payroll file and perform whatever verification procedures he deems necessary. These will include scrutinising masterfile amendments and the period to period reconciliations. He does not have write access to the payroll.

Payment of wages by EFT

* wages are paid to employees by electronic funds transfer. The payroll administrator's computer does not have the bank's EFT software loaded onto it and the administrator is not involved in any way with the transfer, i.e. no access to the bank account, no random number generator device

* once Johan Els is satisfied with the payroll, the same procedures which are followed for making EFT payments for salaries are followed. These are described later in this chapter

* finally, a copy of the payroll is printed out, signed by the payroll administrator and Johan Els and filed in period order. A payslip for each employee is printed and given to the employee. Any queries are dealt with by the warehouse manager and payroll administrator.

5. Payout and deductions

Deductions are also paid over by EFT, or in the case of payments to SARS, by e-filing.

HOW THE SYSTEM WORKS (salaried staff)

1. Introduction

ProRide (Pty) Ltd does not have a large salaried staff so this expense is easy to control. There is no chance of a "fictitious" employee being added or unauthorised increases being effected. Salaries are paid directly into employees bank accounts by electronic funds transfer.

2. Personnel function

As the staff contingent is small, a separate personnel department is not warranted. The wage payroll administrator does not deal with salaries or salaried staff at all. The responsibilities pertaining to human resources are dealt with as follows:

2.1 Appointments

The company uses a reputable employment agency to recruit staff. For example, when Ruth Taylor (purchasing manager) requires a new employee for her department, she is required to prepare a motivation. This will be appraised by Brandon Nel (financial director) who will decide whether the vacancy should be filled. If so, a precise instruction of the qualities, qualifications and experience required by the person to fill the vacancy is prepared. It is signed by the department head and Brandon Nel, and sent to the agency. The agency will prepare a list of up to 3 applicants having conducted extensive background checks and competency tests. The listed candidates are then interviewed by Brandon Nel, Peter Hutton (managing director) and the appropriate department head.

On appointment, the selected applicant is required to sign an employment contract and complete a "Personal Details" form. This form contains inter alia, personal taxation and banking details as well as the starting salary agreed to. The form is signed by the employee

and by Brandon Nel, and becomes the authorising document (masterfile amendment form) for the addition of the employee to the masterfile. A hardcopy personal file is maintained for each employee. All documentation pertaining to the employee is placed in the file and the files are kept under lock and key in a separate filing cabinet by Johan Els (financial manager) for confidentiality purposes.

2.2 Dismissals and resignations

Dismissals and resignations occur very seldom. When they do occur, ProRide (Pty) Ltd consults with their legal advisors to ensure that the law is adhered to.

If a dismissal or resignation does take place then a standard form is completed and signed by Brandon Nel and the employee. This form becomes the authorising document for terminating the monthly salary payment and the (eventual) removal of the employee from the employee masterfile.

2.3 Salary increases

Salary increases occur once a year. Johan Els (financial manager) prepares a schedule which details each employee's current salary as well as their increase history. On the basis of this schedule and performance reviews which are carried out twice a year on each employee, Brandon Nel (financial director) and Peter Hutton (managing director) decide upon salaries for the ensuing year. The schedule is signed by both of them and becomes the authorising document for the increase of salaries on the masterfile. The increases schedule is passed to Johan Els who records the amount and date of each employee's increase on their Personal Details form in their personal file.

3. Payroll preparation

3.1 Procedure

Salaries are paid on the last Wednesday of each month and is a relatively simple procedure as very little changes from month to month. The company uses reputable packaged payroll software which is loaded onto Johan Els the financial manager's PC. The software is menu driven and access is restricted to Johan Els. Having accessed the application, he selects the "prepare payroll" module from the menu. This brings up the payroll for the month on the screen and the opportunity is offered to him to make any amendments necessary. For example

* if a new employee is to be added, he will select the "add employee option" and a sub screen will appear formatted as an employee masterfile record into which Johan Els can key the required data, e.g. employee details, salary, etc. Besides the general programme controls to enhance the accuracy and completeness of data entry such as alphanumeric tests, field size test (on ID number) there are mandatory field checks on, inter alia, the employee's identity number and tax reference number. Without these an employee cannot be loaded onto the masterfile. An employee number is allocated to the new employee by the system

* if an amendment is to be made to an existing employee's record, Johan Nel will call up that employee's masterfile record by entering either the employee's name, or the employee's staff number or the employee's identity number (minimum entry principle). This will bring up a sub screen of the employee's record and Johan Els can make the necessary change, e.g. change in salary or bank details

* if an employee resigns or is dismissed, Johan Nel will carry out the same procedure for calling up the employee's record and enter a specific code and the date of termination. This does not remove the employee's record but does "flag" the record so that from the designated date a salary will not be processed for the individual. The record is not removed from the masterfile because there is information for the year which is needed at the end of the year to be submitted to SARS, e.g. earnings for the year, taxation paid, etc

* using the same procedure, Johan Nel also has the opportunity to make changes which are not changes to the standing data, e.g. a special bonus or a refund of a travel claim or a loan repayment which must be deducted.

The processing of the payroll is carried out entirely by the system without human intervention. The software "imports" the deductions such as PAYE and medical aid contributions, from the relevant tables which are on the system, draws information from the salary employee masterfile and performs the necessary calculations to produce a valid, accurate and complete payroll. All changes to the masterfile are logged and reports of other changes, e.g. bonuses added, travel claims etc, are written to a report. The system also produces a month to month reconciliation of salaries which can be tied back to the logs and reports.

The software which ProRide (Pty) Ltd uses is well supported by the supplier. This is very important because there are a number of variables in any payroll system. For example, rates of PAYE, UIF and other deductions change; this means that the respective tables used to calculate these deductions must be promptly updated. New deductions are introduced from time to time, again making it imperative that the software be updated. ProRide (Pty) Ltd's supplier keeps the software right up to date.

When Johan Els is satisfied with the onscreen version of the payroll, he clicks on the "first confirmation" option. He notifies Brandon Nel (financial director) who calls up the payroll on his terminal for a second confirmation. Before he clicks on the "second confirmation" option, Brandon Nel will access any amendment logs to confirm the validity, accuracy and completeness of any amendments. He will refer, whenever necessary, to the supporting documentation, particularly in the month of salary increases. He cannot, however, make any alterations as he has no write access. Should an amendment be required, he clicks on the "no confirmation" option. The payroll reverts to the control of Johan Els who is then able to make the adjustment. Once Brandon Nel selects the second confirmation, no further adjustments can be made.

3.2 Effecting the transfer

For a full discussion on making EFT payments refer to Chapter 9. In essence the controls over making EFT payments at ProRide are as follows

* the bank has its EFT software loaded on only three terminals at ProRide (Pty) Ltd, one of which is the terminal of Johan Els

* to access the bank's site on the internet a PIN is provided by the bank and a password, unique to the employee wanting to access the site must be entered

* access to the ***functions*** offered by the bank on the site is restricted to a limited number of employees who can access the site in terms of their user profiles, e.g. Dalene Burger, the accounting supervisor can download a bank statement but cannot make an EFT payment

* the bank requires that additional "one time" passwords be entered by employees effecting the transfer. The bank supplies each authorised employee with a random number generator device which is registered to that specific employee by the bank

* salary EFTs must be "authorised" by Johan Els and "released" by Brandon Nel

* once Brandon Nel clicks on the "second confirmation" option the salary software automatically converts the payroll file into a format acceptable to the banks EFT software. This EFT schedule contains only the employees name, bank details and the net amount to be transferred. The abridged payroll (EFT schedule) appears on screen for a final check by Johan Els. He selects the "authorise" option. To effect the transfer Brandon Nel must then click on the "release" option (second signatory

principle). Both the "authorise" option and the "release" option require that the "one time" passwords be entered

* selection of the "release" option initiates the transfer from the bank's main account, of the total amount of the salaries into ProRide (Pty) Ltd's salary account, and from there to the bank accounts of each employee.

3.3 After the transfer

* audit trail: the following day Johan Els downloads a copy of the bank statement for the salaries account. Only he has access to this particular statement for confidentiality purposes. He compares the bank statement to a hard copy version of the EFT payment schedule to confirm that the correct amounts were transferred. Any problems will be resolved. For example, on occasion an employee will change his bank account and forget to inform ProRide (Pty) Ltd, and the EFT will not go through. The monthly bank statements and EFT schedules are filed in date order in his secure filing cabinet

* payslips: the salary software prints out a monthly payslip for each employee which provides details of the monthly earnings, pension contributions and deductions as well as cumulative totals year to date.

4. Deductions

The payroll software produces schedules of all the deductions which must be paid over to the relevant authorities e.g. PAYE, medical aid and pension contributions. These are paid by EFT (normal controls apply) and by e-filing in the case of payments to SARS.

Note : exactly the same principles apply to the payment of wages by EFT. One difference is that Johan Els does not have write access to the wages payroll file and any changes required which were picked up after the payroll administrator has confirmed the payroll (first confirmation), will have to be referred back to the payroll administrator. Johan Els cannot effect the changes.

AUDITING THE CYCLE

1. INTRODUCTION

For the purposes of this section we have not dealt with the payment of salaries and wages as separate expenses as they are so similar in nature. However, there are a few differences which may affect the audit.

* The underlying controls will basically be the same with the general exception that for wage earners gross remuneration will not be fixed as it is for a salaried employee. There will be controls over recording the hours worked, both normal and overtime for wage earners, and the auditor will want to be satisfied that these controls result in the accurate and complete recording of hours worked.

* Directors and prescribed officers of the company are salaried employees, and extensive disclosure of their remuneration must be made in the annual financial statements. The audit of salaries will include procedures relating to these disclosures.

The risk of material misstatement in the salaries and wages accounts would not normally be regarded as high even if they make up a significant portion of the company's expenses. The reasons for this are

* Management is usually strongly control conscious with regard to the payment of salaries and wages as it is a cycle which can result in fraud if controls are not implemented.

* The account headings do not offer huge opportunities for the directors to manipulate the financial statements if they are inclined to do so.

* There are parties external to the entity, which are directly "interested" in the cycle, e.g. SARS, the company's medical aid, trade unions, etc, so for example, trying to include fictitious employees can get complicated. Government departments such as the Department of Labour may also conduct external audits of the company's employment practices.

* Current payroll software processes are accurate and contain programme controls which make it difficult to include fictitious workers or change salaries or wage rates without leaving a trail, e.g. mandatory fields and logging of amendments.

However, the auditor cannot just assume that the above applies! There are plenty of wage frauds, management is not always honest, companies don't necessarily use good software (or any software!), and there are plenty of illegal labour practices being undertaken.
In terms of ISA 315 (Revised), the auditor is required to identify and assess the risk of material misstatement in the financial statements and it is this process which will determine the nature, timing and extent of the further audit procedures which will be carried out on the audit. There are a number of circumstances which could give rise to material misstatement relating to salaries and wages which the auditor may need to address

* ***The inclusion of fictitious employees on the payroll.*** Although the inclusion of fictitious employees is far more likely to be a fraud perpetrated by employees to enrich themselves and not an attempt by management to manipulate the profits of the company to reduce tax, the auditor will still need to respond if he thinks the risk is present. This is made clear in ISA 240. We quite frequently read of auditors from the Auditor General's office, uncovering "ghost/dummy" workers (including teachers) in provincial and government departments, so the threat of this practice is real. On the audit of smaller companies, there is always the possibility of owners/directors/managers deliberately adding a family member/friend to the company payroll even though the individual does not actually work for the company. Remember that a fictitious employee does not have to be an imaginary person – a fictitious employee in the context of a company may be a genuine person who is paid by the company but who does not work for the company.

* ***Illegal employment practices.*** These include employing illegal aliens, people without work permits, or paying wages below the minimum wage rates. Whilst wages (and salaries) paid in these circumstances may not directly result in the misstatement of the financial statements, there are severe penalties and fines arising from these illegal activities. To achieve fair presentation these should be disclosed but it is hardly likely that the directors will make these disclosures! In addition, these practices would amount to a reportable irregularity in terms of Section 45 of the AP Act 2005. Whilst illegal employee practices can be an emotive and ethical issue, the fact remains that they are illegal and the company could face prosecution, penalties and fines. The problem is compounded by the fact that management are unlikely to include these individuals on the formal payroll and wages paid to them may be concealed.

* ***Disclosure of director's and prescribed officer's remuneration.*** In terms of Sec 30 of the Companies Act 2008, extensive disclosures about the remuneration of directors and prescribed officers in all its forms, must be made in the financial statements of all companies which in terms of the Act, have their financial statements audited. Directors, particularly of private companies, may be hesitant/unwilling to comply with these requirements which may result in disclosure which is incomplete or inaccurate. An added complication is that the definition of a prescribed officer is open to interpretation as to which employees are or are not prescribed officers, which may also result in incomplete disclosure in terms of the section. The risk of material misstatement in disclosure may be increased if the directors engage in tax evasion schemes to reduce their personal tax burdens. For example, the company provides vehicles for the director's personal use, pays all vehicle expenses, but the company does not declare the fringe benefit and does not deduct PAYE. This can also amount to a reportable irregularity in terms of the AP Act 2005.

* ***Employment benefits.*** Furthermore, in terms of various accounting standards there are extensive disclosures which must be made in respect of employee benefits which apply to both salary earners and wage earners. These are classified as either short-term benefits, long-term benefits, post-employment benefits and termination benefits, and can be in themselves very complex to account for. The audit of amounts and disclosures relating to these benefits, is beyond the scope of this text and will not be addressed other than in a general way.

2. ASSERTIONS

2.1 Transactions

The payment of a wage or a salary is a transaction, so the relevant assertions which the auditor will address are

* ***occurrence***, i.e. the totals (account balances) recorded for salaries and wages include only amounts paid to genuine (non-fictitious) employees in respect of genuine (non-fictitious) hours worked.

* ***completeness***, i.e. all salaries and wages paid or payable for the period, have been included in the account balance. The risk of material misstatement arising from the omission of salaries or wage payments is not usually anything other than low, but the auditor should be aware that payments to illegal employees may be excluded and written off through other accounts.

* ***accuracy, cut-off and classification,*** i.e. amounts paid for salaries and wages and other related data have been recorded appropriately, the payments have been recorded in the correct accounting period, and the amounts have been recorded in the proper accounts. The risk of material misstatement relating to these assertions is usually low. Because the use of packaged salary and wage software is widespread, the accuracy of calculating amounts owed is usually very accurate and postings to the proper accounts (e.g. salary expense, deduction account, etc) are appropriate. With regard to cut-off, there is a possibility that at the end of the financial year there may be amounts due to employees in respect of salaries or wages. For example, if wages are paid every two weeks and the financial year falls in the middle of that two week period, there will be a week's wage owing at the financial year end which must be accrued.

2.2 Presentation and disclosure

As pointed out above, the risk of material misstatement in the disclosure of director's and prescribed officer's emoluments may be reasonably high. The auditor is most likely to be concerned about the following assertions

* ***completeness,*** e.g. have all disclosures about all directors (executive and non-executive) and all prescribed officers, been included.

* ***classification and understandability,*** e.g. does the disclosure classify the type of remuneration as required, e.g. salary, contribution to pensions, compensation for loss of office, etc, and have disclosures been expressed clearly.

* ***accuracy and valuation,*** e.g. are the details of the disclosure and related amounts accurate and fair.

3. FURTHER AUDIT PROCEDURES

The nature, timing and extent of the further audit procedures to be conducted, will depend on the risk assessment which was carried out. Audit firms use different combinations of procedures which may include some or all of the following :

3.1 Analytical procedures

Where the risk of material misstatement is assessed as low, the auditor may simply decide to conduct analytical procedures and follow up on any fluctuations revealed by the analysis. Analytical procedures will include

* comparisons
  - salaries : month to month by division, department or section
  - wages : period to period by cost centre, etc.
  - salaries and wages to the prior year corresponding period
  - deductions paid over to third parties, month to month.

* ratio and trend analysis, e.g.
  - salaries as a percentage of total expenses
  - wages as a percentage of production costs
  - wages in relation to production (output).

* investigation of fluctuations and follow up of any explanations given by the client.

* if a month to month reconciliation for salaries and a period to period reconciliation for wages are produced, they will prove a valuable source of evidence for the auditor as they should corroborate the fluctuations identified by the analytical procedures. They should also provide an explanation for the fluctuations. For example, the reconciliation may reveal that an increase in net salaries arose due to the appointment of ten new staff members. The auditor would then confirm this by inspection of the supporting documentation, e.g. employment contracts, signed masterfile amendments, etc.

3.2 Procedures to confirm that employees on the payroll are not fictitious

The auditor's intention will be to obtain evidence that salaries/wages are paid to genuine living people who ***work for the company***. To do this, the basic approach will be to extract a sample of employees from the payroll selected, and

* Inspect the documentation in the employee's personnel file, e.g. signed employment contract, identity details (identity numbers can be verified on the national identity number database), tax registration forms, etc. and agree it to the payroll.

* Perform a positive (physical) identification of the employee where possible; this would involve visiting the employee at his place of work during working hours and inspecting his personal identity document or staff identity tag.

* Enquire of senior personnel to confirm (in writing) that specified individuals are employed in their section or division.

* Inspect returns to outside entities for the inclusion of employees selected in the sample, e.g. PAYE reconciliations submitted to SARS, or medical aid contribution returns.

* Use audit software to scan the employee masterfile for "error conditions" which may indicate fictitious employees, e.g.
  - duplicated or missing identity numbers
  - duplicated or missing tax reference numbers
  - duplicated bank accounts
  - duplicated staff employee numbers.

* By discussion with the staff in the personnel section and examination of the employment and dismissal/resignation documentation, confirm that employees are put onto or removed from the masterfile on the correct date (if an employee leaves, but is left on the payroll, he is in effect a fictitious employee).

3.3 Detailed testing of the payroll

The results of analytical procedures are only worthwhile if the underlying data which is being used in the analysis, is valid, accurate and complete. In the context of conducting month to month or period to period comparisons, the auditor may wish to satisfy himself that the salary or wage data against which he is comparing other salary or wage data, is correct. An approach which can be used by the auditor, is to select the payroll for a base period and carry out detailed tests for that period on the payroll. If the auditor is satisfied with the "correctness" of the base period, a combination of analytical review procedures and working with the period to period reconciliations, should provide the auditor with suitable evidence relating to salaries and wages paid. The auditor's objective will be to satisfy himself that

* employees on the payroll are genuine employees (this relates to the occurrence assertion and has been addressed in 3.2 above)

* the gross salary used in the calculation of the net salary paid, was authorised or

* in the case of wages, the hours worked (normal and overtime) and the hourly rates used in calculating the gross wage were authorised, and the calculation was correct

* the standard contributions by the company to medical aid and pension funds etc, and the corresponding deductions from the employee's earnings are correct

* all additional amounts paid to the employee and deductions made, e.g. commissions, bonuses, travel claims or loan repayment deductions, were authorised

* the calculation of the net pay is correct.

To conduct detailed tests on the payroll, the auditor should

* confirm that the gross salary used in the payroll is authorised in terms of company's remuneration policies and signed salary notifications in the employee's personnel file

* trace any additional amounts paid to the employee to source documentation and

  - inspect the source documentation for a valid authorising signature, e.g. the financial director approving the payment of an incentive bonus or the sales manager authorising a sales commission

- reperform any calculations
- confirm by enquiry and inspection, that the payment is valid in terms of company policy

* for hourly paid employees, confirm that the hourly wage rate used for the employee is in accordance with the wage rate for that level of employee and is authorised in terms of a notification in the employee's personnel file or a general agreement with a trade union or similar, if applicable

* for hourly paid employees, inspect any overtime reports signed by the foreman or production manager for the period selected, and confirm that the rate used for overtime complied with company policy and labour requirements, e.g. overtime rate is normal time and a half

* compare all deductions, e.g. PAYE, pension, medical aid, to the appropriate tables/rules to confirm that the correct amounts were deducted

* confirm by inspection, that all non-standard deductions, e.g. garnishee orders or loan repayments, are supported by approved documentation

* test the casts and the arithmetical accuracy of the payroll as appropriate

* trace amounts posted from the selected payroll to the relevant accounts in the general ledger.

3.4 Presentation and disclosure

The presentation and disclosure of information pertaining to the payroll cycle will be governed by

* the requirements of Sec 30 of the Companies Act 2008 (applicable to the remuneration of directors and prescribed officers for any company which is required to be audited in terms of the Cosact)

* the JSE listing requirements (for listed companies)

* the King III Report on corporate governance, and

* a number of accounting statements, e.g. IAS 1, IAS 19, IAS 24, IAS 37.

Usually the client will provide detailed workings/schedules to support the actual disclosures in the financial statements and a senior member of the audit team will

* by inquiry and inspection, evaluate the company's processes for gathering this information

* by inquiry of senior personnel, inspection of internal and external documentary evidence, recomputation of calculations, etc

gather sufficient appropriate evidence that all disclosures required in terms of the pronouncements listed above, have been made, classified correctly, and that amounts are accurate and fairly valued and that the disclosures are made in an understandable manner. This will include determining exactly which "prescribed officers" must be included in the remuneration of directors' disclosures.

3.5 Notes

Note 1. If the auditor suspects there are wages being paid which are not being recorded in the payroll records, e.g. to workers who do not have work permits, he should

* discuss the matter with senior company personnel, e.g. financial director, personnel manager and/or lower level employees such as foremen

* consider conducting a reverse identification (e.g. employee to payroll records)

* be alert to situations which suggest that there may be such practices going on, e.g. the labour costs do not appear to match up with the size of a construction project being undertaken by a company

* be alert for regular cash payments flowing out of the company.

Since this type of practice carries strong penalties, and is unlikely to be carried out without the knowledge of at least some senior personnel, it may be very difficult to follow up on.

Note 2. Attendance at wage payouts.
Before the strong move towards paying wages by EFT took hold, wages were generally paid in cash with employees attending a wage payout at a central point where they were required to present some form of identification and sign the payroll to acknowledge receipt of the pay packet which contained the cash they were due. Any unclaimed wages were entered in an unclaimed wage register, kept in a safe place, and paid over to the employee when he returned to work. Refinements of this system included using security companies to actually make up the pay packets and assist with the payout of the wages. It was a common practice for trainee accountants to attend a wage payout on a ***surprise basis*** as this provided an opportunity to verify the existence of employees on the payroll and identify any potential fictitious employees evidenced by pay packets which were not collected or by employee names which remained unsigned on the payroll. Obviously with the considerable increase in the payment of wages by EFT, attendance at a wage payout is no longer a common procedure for a trainee accountant. However, enquiries relating to the update of this text, revealed that auditing firms are from time to time requested to attend wage payouts. Examples given were typically as a direct request from a client to attend a payout at a remote site, e.g. a commercial farming operation, plantation or construction site, more as a control procedure for management, or as an investigation into a suspected wage fraud, rather than a procedure carried out for audit purposes. The basic policies and principles for attending a wage payout under these circumstances would be

* attendance would be on a surprise basis, i.e. those responsible for the payment of wages at the client's site, should not be aware of the auditor's attendance
* the number of pay packets and basic details of the employees to be paid would be agreed to the payroll before the payout takes place
* the identification presented by the employee, should be inspected and marked by the attending auditor before the pay packet is handed over (identification may be difficult!)
* the employee should sign the payroll under the supervision/observation of the auditor
* at the conclusion of the payout the auditor should reconcile the unclaimed pay packets with the unsigned employee names on the payroll, and create a detailed workpaper
* the identity of all employees who did not collect their pay packets, will be followed up to determine whether they are fictitious
* the auditor should perform these tasks in the presence of the person administering the payout and should ensure that the auditor is not left alone with the pay packets.

Note 3. ***Period to period wage reconciliation*** – Example (gross amount and headcount only)

Period 1 – Gross (R172 900)

95 employees x 40 hrs x R35 per hour	R133 000
95 employees x 8 hours x R52.50 per hour (overtime)	R 39 900
	R172 900

Period 2 – Gross (R142 800)

102 employees x 40 hrs x R35 per hour	R142 800
Difference (between period 2 and period 1)	(R30 100)
Decrease in overtime	R 39 900
Increase in employees : 7	(R 9 800)

Period 3 – Gross (R181 816)

104 employees x 40 hrs x R38.50 per hour	R160 160
25 employees x 15 hrs x R57.75 per hour (overtime)	R 21 656
	R181 816
Difference (between period 3 and period 2)	R 39 016
Increase in employees 2 x 40 x R38.50	R 3 080
Wage rate increase 102 x 40 x R3.50	R 14 280
Increase in overtime	R 21 656
	-

Head count reconciliation

Number of employees : period 1	95
Add appointments : start of period 2	7
Number of employees : period 2	102
Less: resignations end period 2	(4)
Add appointments: start of period 3	6
Number of employees: period 3	104

Note: all appointments and dismissals must be supported by authorised documentation. This is a simple illustration of the reconciliation. In practice a period-to-period reconciliation will be far more complex particularly for a large work force.

CHAPTER 14

FINANCE AND INVESTMENT CYCLE

CONTENTS

		Page
THE ACCOUNTING SYSTEM AND CONTROL ACTIVITIES		
1.	Introduction	14/2
2.	Characteristics of the cycle	14/2
3.	Compensating controls	14/3
4.	Fraud in the cycle	14/3
THE FINANCE AND INVESTMENT CYCLE AT PRORIDE (PTY) LTD		14/4
THE AUDIT OF THE CYCLE		14/6
AUDITING FAIR VALUE		14/7
AUDIT PROCEDURES - THE FINANCE CYCLE		
1.	Share capital	14/8
2.	Debentures	14/9
3.	Long-term loans	14/11
4.	Finance lease liabilities	14/11
5.	Provisions, contingent liabilities and contingent assets	14/14
AUDIT PROCEDURES - THE INVESTMENT CYCLE		
1.	Property, plant and equipment	14/18
2.	Investments in shares	14/25
3.	Long-term loans made by the company	14/27
4.	Intangible assets	14/29

THE ACCOUNTING SYSTEM AND CONTROL ACTIVITIES

1. INTRODUCTION

This cycle essentially deals with those transactions which a company enters into to raise finance, for example by issuing shares, or borrowing money from a bank or investment company. The cycle also deals with the investments the company makes, whether it be in property, plant and equipment, making long-term loans or investing surplus funds. The transactions in this cycle will usually result in the creation or alteration of an account balance, e.g. investment in property, plant and equipment, but may also result in cash inflows and outflows which are written off at the end of the financial year, e.g. interest or dividends received on investments or interest paid on borrowings. In a general sense the audit of the capital employed section of the statement of financial position is linked to the finance side of the cycle, and the audit of non-current assets to the investment side of the cycle.

2. CHARACTERISTICS OF THE CYCLE

2.1 Frequency of transactions

The number of transactions in this cycle is considerably smaller than for "every day" transactions such as purchases and sales, salaries and wages etc.

2.2 Size of transactions

Transactions in this cycle are usually material. Generally when a company raises finance or purchases non-current assets, the amounts are large.

2.3 Legal and regulatory requirements

Transactions in this cycle are frequently governed by statute and by the company's Memorandum of Incorporation. For example if the company chooses to issue shares it must comply with the requirements of the Companies Act. If the directors wish to declare a dividend to shareholders they must comply with the company's MOI and with Sec 46 of the Companies Act, which deals with distributions (as defined) to shareholders.

2.4 Non-routine internal controls

Due mainly to the three characteristics identified above, transactions in the cycle will not be subjected to the routine every day controls relating to transactions. However, it is still very important that strict controls are exercised over these transactions and what might be termed "compensating" controls should be put in place. These are discussed below (para 3).

2.5 Non-standard documentation

Because of the "uniqueness" of transactions in this cycle it is unlikely that the documentation relating to them will be the standard everyday documentation, e.g. goods received notes, invoices etc. Certainly there will be occasion when these documents are used but more often than not, documents specific to a particular type of transaction will be used, such as contracts and lease agreements.

2.6 Major risks within the cycle

Although the risk of material misstatement must always be evaluated in terms of the specific circumstances at the client, generally the major risks would be that the client understates ***completeness*** of the long term liabilities or overstates ***existence*** and ***valuation*** of the investments which have been made whether these are investments in plant and equipment etc, or in other private or public companies. Due to the legal and regulatory requirements there is also a risk that invalid transactions have ***occurred***, e.g. long-term loans raised in contravention of the Memorandum of Incorporation, or the issue of shares to a director without the appropriate approval in terms of the Companies Act.

3. COMPENSATING CONTROLS

3.1 Planning

Transactions in this cycle, e.g. investment in plant and equipment, should be carefully planned by senior experienced management. This normally involves:

* the formation of specific committees. e.g. a capital expenditure committee, which will evaluate the need for capital expenditures and how they will be financed, or an investment committee, which may look at alternative forms of investment for surplus funds.
* the preparation of capital expenditure budgets and cash flows.
* exhaustive consideration of alternatives e.g. best method of raising finance.
* regular comparison of actual performance to budgeted performance to assist in ongoing planning.

Note : decisions will often be prompted by strategies adopted by these committees to respond to risk.

3.2 Authorization

Authorization of material finance and investment transactions should be at the highest level, e.g. the board of directors, and may be subject to authorization requirements in the company's MOI and the Companies Act where applicable.

3.3 Implementation

Where the implementation of the transaction is other than straightforward, it should be carried out by competent staff and properly controlled. For example, the installation of a new production line should be regarded as a project and sound project controls must be implemented. If a public share issue is to be undertaken, merchant bankers, lawyers and other experts should be involved.

3.4 Review and approval

Transactions in this cycle should be subjected to:

* progress reporting
* comparison to plans and budgets
* independent scrutiny by internal audit particularly for compliance with legal and regulatory requirements.

4. FRAUD IN THE CYCLE

4.1 Fraudulent Financial Reporting

This cycle presents the directors with a fair number of opportunities to report fraudulently as there are numerous account headings which can be manipulated. Of particular concern for the auditors would be the manipulation of allowances, provisions, impairments and fair values. Working on the assumption that the directors motive would be to improve the financial statements by reporting fraudulently, the following methods could be adopted:

* ***creating unjustified reserves with a corresponding increase in fixed assets*** (valuation), e.g. obtaining an inflated property valuation from an estate agent.
* ***omitting long term liabilities*** (completeness) e.g. failing to record a new loan and disguising the inflow of cash as income, or failing to capitalize finance leases.
* ***undervaluing long-term liabilities*** (valuation) e.g. failing to amortise debentures redeemable at a premium.
* ***overstating property, plant and equipment etc by including fictitious assets or assets which the company does not own*** (existence and rights) e.g. including the assets of a related party.
* ***overstating plant and equipment, vehicles etc by understating depreciation allowances and impairments*** (valuation) e.g. failing to write down obsolete/impaired machinery.
* ***overstating investments in listed and/or private companies*** e.g. failing to write down the cost of investments in private companies, where the fair value of the investment has fallen.

* ***understating or omitting provisions/allowances*** e.g. not providing for long-term environmental damage which the company has an obligation to rectify.
* ***omitting or inadequately disclosing contingent liabilities*** e.g. the company makes no mention in the notes of a pending lawsuit which may have grave consequences for the company.

Remember also that any manipulation of the statement of comprehensive income by the directors will also affect the capital section of the statement of financial position.

4.2 Misappropriation of assets

This cycle does not present any unique opportunities to management or employees to misappropriate assets other than:

* ***making unauthorized use of the company's assets for personal use*** e.g. using the company's computer processing facilities to run private accounting jobs; taking company vehicles or equipment home at the weekend for private use; using company assets as security for personal loans; or the directors making (unauthorized) long-term loans to themselves.

THE FINANCE AND INVESTMENT CYCLE AT PRORIDE (PTY) LTD

1. INTRODUCTION

As with many businesses of the size of ProRide (Pty) Ltd, there are not many "finance and investment" decisions made in a single year. However, this does not mean that controls are weak in the cycle – on the contrary. Finance and investment decisions are subject to a full range of compensating controls and other controls.

2. PLANNING

2.1 Budgets

All transactions in this cycle are carefully planned. The annual budget forms the basis of planning. In putting together their annual budgets, department heads (e.g. Reg Gaard, warehouse manager, Gary Powell, IT manager) must indicate and motivate for any new capital expenditures they require. As part of their motivation they must obtain estimates (quotes) from various suppliers on price, and any service contract costs. For example, should Reg Gaard require a new forklift, he must present quotes from three suppliers.

All capital expenditure is subjected to the same budgetary process regardless of the value i.e. department heads are ***not*** given permission to make acquisitions up to say, R10 000 without committee consent.

2.2 Capital expenditure committee

This committee consists of Brandon Nel, Johan Els and Peter Hutton, the financial director, financial manager and managing director respectively. All motivations from department heads are evaluated in the presence of the department head so that alternatives can be discussed and queries resolved.

The decision as to whether or not to go ahead with the expenditure is minuted along with the full detail of the proposed expenditure. The minute is signed by the committee members and becomes the authority for the acquisition.

2.3 Financing

All three members of the committee have financial qualifications and are quite capable of deciding on the best method of financing the purchase. Where they require any particular expertise with an asset financing decision, they will obtain assistance from their bankers and external auditors.

3. AUTHORISATION AND IMPLEMENTATION

The acquisition of the asset becomes the responsibility of the department head working with Brandon Nel, the financial director, who is solely responsible for negotiating final prices, terms and finance arrangements. Any contracts entered into are signed by Brandon Nel. No material purchase agreement/financing contract is drawn up without it being scrutinised by the company's legal advisors.

4. REVIEW AND APPROVAL

As the incidence of capital expenditures is low, there is limited review and approval. However, about once every three months the committee will meet to discuss whether

* acquisitions scheduled in the capital budget have actually been acquired and are functioning as required.
* business circumstances which necessitate a change to the budget have occurred, e.g. capital expenditure should be delayed because cash flow has not been as expected, or an expected increase in inventory holding has given rise to a need for new warehousing facilities.
* equipment etc is being adequately maintained.

5. OTHER CONTROLS

5.1 The department heads are responsible for the maintenance of assets in their section – e.g. ensuring that, where applicable, they are serviced at the appropriate time.

5.2 Company assets may not be used by employees for personal purposes.

5.3 Payments, whether they be by instalment or "one off" payments, are subject to the same control procedures as all other payments (see chapter 11).

5.4 A fixed asset register is kept and once a year a physical asset count is undertaken. Every fixed asset is inspected and traced to the fixed asset register, and its condition assessed.

6. INVESTMENT OF SURPLUS FUNDS

As ProRide (Pty) Ltd is a private company, decisions on how profits which are surplus to business requirements should be treated, are resolved by a meeting of the shareholders. Both Brandon Nel and Peter Hutton are shareholders. As a policy the company does not make investments in listed or private companies; shareholders prefer to declare dividends and make investments in their private capacities.

7. LONG TERM LOANS

The company has a policy that no long term loans will be made to anyone, other than the directors. Loans to directors are made very seldom and are only made

* up to specified limits (a percentage of the director's annual remuneration)
* on the strength of a written motivation
* if ***all*** shareholders agree.

THE AUDIT OF THE CYCLE

1. As for all other cycles, ISA 315 (Revised) requires that the auditor identify and assess the risk of material misstatement at the financial statement level and at the assertion level for classes of transactions, account balances and disclosures. The risk assessment procedures will be those which are carried out in any cycle and will hinge around the auditor gaining a thorough understanding of the entity and its environment. In the context of this cycle, the auditor will need to evaluate whether there is anything in the assessment of risk at financial statement level which may filter down into the audit of the cycle and whether there are any specific risks pertaining to the various balances and transactions in the cycle. For example :

* at financial statement level : if the auditor has concerns about the "accounting" competence of management, there may be a risk of material misstatement in a number of balances relating to the cycle, e.g. management may not even be aware of matters such as impairment requirements to establish fair value, or how intangible assets should be measured
* at account balance level : risk assessment procedures may have revealed that a number of machines may have become technically obsolete
* at transaction level : risk assessment procedures may reveal that long-term loans are being made to directors and other related persons without considering the requirements of the Companies Act.

2. ***Overall responses to risk of material misstatement at financial statement level***

In terms of ISA 330, the auditor must implement overall responses to address the risk of material misstatement at the financial statement level. For example

* assigning more experienced staff to the audit team, e.g. in response to an assessed risk that management may lack "accounting" competence, the auditors will assign staff who have a high level of technical competence relating to the account headings in this cycle
* providing more supervision of audit work as well as more frequent and comprehensive review
* the engagement of an expert to assist with the audit of complex transactions.

3. ***Responding to risk at assertion level***

There is no change in principle here. The auditor will still need to decide on the nature, timing and extent of tests which will reduce audit risk to an acceptable level. As was explained in Chapter 6, the best mix of tests of controls and substantive tests, i.e. observation, reperformance, inspection etc must be decided upon and executed. Particular considerations for these cycles include:

3.1 ***Nature***

* as there are normally only a few transactions (relatively) in this cycle, the auditor may limit tests of controls (not ignore them!) and concentrate on performing substantive tests of detail, often on each of the transactions that have occurred, and the account as a whole.
* a common approach is to verify the opening balance on the account, vouch the transactions which make up the movement on the account including adjusting journal entries, and verify that the closing balance agrees with and is appropriately reflected in the financial statements. For example, let us assume that the company has raised two long-term loans and repaid one. Broadly it will be audited as follows:

Opening balance :	compare to prior years closing balance in working papers
Two new loans :	vouch as transactions (occurrence, accuracy, cut-off, classification and completeness)
Repayment :	vouch as a transaction (occurrence, accuracy, cut-off classification and completeness)
Closing balance :	cast account and confirm that appropriate presentation and disclosure has been achieved.

Where a subsequent measurement adjustment has been passed, for example for the amortisation of a debenture redeemable at a premium, the adjusting journal entry will be vouched.

If there are numerous and frequent transactions in this cycle e.g. lots of purchases of machinery and other equipment, then tests of controls would be carried out as with any other cycle. The same broad approach would he adopted, but the extent of substantive testing would be influenced

by the outcome of the tests of controls, and samples of transactions relating to the account heading would be extracted for audit.

3.2 Extent

* As indicated there are frequently few transactions in the cycle and each one can be audited individually. When there are numerous transactions, e.g. in very large organisations, the normal principles of sampling would be adopted, and the extent of substantive testing would be influenced by the risk assessment and effectiveness of controls.

3.3 Timing

* There is nothing about the cycle itself which makes the timing of tests particularly critical so they may be conducted at the interim or final stage. Quite often the external auditor may be asked for input at the time the transactions are taking place, e.g. the auditor may be consulted on Companies Act or JSE listing requirements for a share issue and some audit work may be done at this stage. Where a tight audit deadline is in place, early verification and roll forward procedures can take place quite conveniently, e.g. physical asset inspections, statutory work, scrutiny of finance leases raised at an interim date two months prior to year end.

AUDITING FAIR VALUE

It is quite possible that in this cycle "fair values" will be used extensively. In some cases e.g. for investments in listed shares, auditing fair value is straightforward. The auditor can make use of share price listings which are widely available, but for other account headings relating to this cycle, establishing fair value may be far more complex.

Although ISA 540 – Auditing accounting estimates, including fair value accounting estimates and related disclosures, deals in part with auditing fair values, the following ten points provide a solid basis for understanding the requirements of auditing fair value. They are derived from a former ISA which was subsequently withdrawn.

Auditing more complex fair values will in general, require that the auditor:

* obtain an understanding of the entity's process for determining fair value measurement and the relevant control activities, sufficient to identify and assess the risk of material misstatement at assertion level.
* evaluate whether the fair value measurements and disclosures in the financial statements are in accordance with the International Accounting Standards.
* where the "intention" of the directors is an important criterion in how an asset/liability is measured and disclosed, for example, whether investments in shares are speculative or are to be held in the long term, the auditor should
  - consider management's history in carrying out its stated intentions
  - review written plans and other documentation e.g. minutes relating to an investment in shares, budgets etc, to clarify and confirm management's intentions
  - consider the logic and reasonableness of management's reasons for choosing a particular course of action
  - consider management's ability to carry out an intended course of action.
* evaluate whether the entity's method for its fair value measurement is applied consistently.
* comply with ISA 620, where he (the auditor) has engaged an expert to assist in the audit of fair value.
* where the measurement of fair value includes the use of assumptions, forecasts etc, e.g. the valuation of a private company, evaluate whether
  - the assumptions are reasonable
  - an appropriate valuation model was used
  - the underlying data was relevant and reliable
* perform audit procedures on data used for fair value measurement and disclosure to determine that it is accurate, complete and relevant.
* consider the effect which any subsequent events may have on fair values.
* obtain written management representations pertaining to fair values used e.g. the reasonableness of significant assumptions.
* if applicable (e.g. where there is significant use of fair values), discuss the fair values with those charged with governance.

AUDIT PROCEDURES - THE FINANCE CYCLE

1. SHARE CAPITAL

We will only consider the issue of share capital by private companies, as the statutory and JSE requirements relating to public and listed companies are fairly onerous and a description of these requirements is beyond the scope of this text.

1.1 Opening balance

* inspect prior year workpapers and prior year financial statements to confirm that the opening balance agrees with the prior year closing balance.

1.2 Occurrence

* inspect the Memorandum of Incorporation and any relevant shareholder resolutions:
  - for any conditions with which the issue must comply,
  - to establish that the company has the necessary ***authorised*** (but unissued) share capital to make the issue, (note, the board may resolve to issue shares at anytime but they must be authorized shares and the MOI may include conditions).
* if any shares were issued to the directors (or a person related to the director or a nominee of such director) inspect the minutes of meetings of shareholders for a ***special*** resolution approving the issue to the director. Note, in certain circumstances this authority is not required, e.g.
  - where the director is exercising a pre-emptive right
  - the issue is made in proportion to existing holdings on the same terms and conditions as has been offered to all shareholders of the company or to all shareholders of the class of shares being issued.
* confirm by inspection of the minutes of the meetings of shareholders, communications with the shareholders, or inquiry of the directors that the requirements relating to any pre-emptive rights (to the new shares) were satisfied.
* inspect the minutes of meetings of directors to confirm that
  - the resolution to issue shares was approved
  - the issue price of the shares was for an "adequate consideration" determined by the board (Sec 40)

Note: in terms of the Companies Act 2008 par value shares cannot be issued.

Note: meetings must be quorate and approval must be in terms of the Companies Act 2008 (and MOI) for ordinary and special resolutions.

* inspect the register of shareholders and agree details to the share capital account in the general ledger/statement of financial position, noting that the addition of new shareholders and changes to existing shareholdings agree with the minutes.
* trace the receipt of payment for the shares to the cash receipts journal and bank statement or inspect appropriate evidence of value received by the company if the consideration received for shares was other than cash.

1.3 Completeness

* confirm with the directors that no other share issues have taken place during the current year.

1.4 Accuracy, cut-off, classification

* reperform the calculations to verify that the consideration received for the shares is in accordance with the issue price as authorised (accuracy).
* confirm by inspection of dates on the supporting documentation that the issue took place during the accounting period under audit (cut-off).
* cast the capital account and all related documentation.

1.5 Closing balance

* trace the closing balance stated capital account to the financial statements (balances will be reflected in the "changes in equity" note).

1.6 Assertions pertaining to presentation and disclosure

* the auditor must inspect the disclosures in the AFS and consider whether
  - they are complete in terms of the applicable accounting framework, e.g. the following are disclosed for each class of share
    - the number of shares authorised and issued
    - the rights, preferences and restrictions attaching to that class of shares
    - details of shares issued to directors
    - details of authorized but unclassified shares
  - they are consistent with evidence gained on the audit
  - amounts, facts, dates etc are accurate and agree with the evidence gathered
  - any classification of the information disclosed is appropriate
  - the wording of disclosures is clear and understandable.

2. DEBENTURES

The audit of debentures, which are regarded as loan capital, attracts a mix of procedures similar to the audit of share issues and long-term liabilities. Again we deal only with the issue of debentures in a private company. If debentures are offered to the general public, it is almost like a share issue and is controlled by the relevant Companies Act sections, including the issuing of a prospectus.

2.1 Important accounting aspects

IAS 39 – Financial Instruments : Recognition and Measurement, requires that debentures are held at amortised cost. An auditor should bear this in mind when, for example auditing a debenture which is redeemable at a premium. IAS 39 requires the use of an effective interest rate in order to correctly reflect the value of the debenture at each reporting date and the finance cost associated with it.

In terms of IAS 39, the effective interest rate is the rate that "exactly discounts estimated future cash payments through the life of the financial instrument". Transaction costs may be included in this calculation. In effect the true finance cost (interest plus premium) is calculated and spread over the life of the debenture.

Basic example : compulsory redeemable debentures

An entity issues 100, R10 par value debentures on 1 January 0001
Coupon rate 10%, Redeemable at R12 on 1 January 0004
Effective Interest Rate is 15.72% (given)

Working	***Effective int.***	***Interest payment***	***Capital***
	R	***R***	***R***
1 Jan 0001			1000
31 Dec 0001	157	(100)	1057
31 Dec 0002	166	(100)	1123
31 Dec 0003	176	(100)	1200

Based on this working

* at 31 December 0001, the debenture will be reflected at R1057 and the journal entry to record the finance charges would be:

Dr Finance Costs	R57
Cr Debenture account	R57

* at 31 December 0002 the debenture would be reflected at R1123 and
* at 31 December 0003 at R1200 (the amount to be repaid the next day)

Note 1 : The interest payment of R100 and premium will give a total finance cost of R157 in year 1, R166 in year 2 and R176 in year 3.

Note 2 : This example is kept simple for the purposes of explaining the principles of auditing a straightforward compulsory redeemable debenture (see below). An auditor may be required to audit more advanced transactions, e.g. compulsory convertible debentures. The important thing to remember is that the transaction/account heading being audited must be tested for

compliance with all relevant financial reporting standards. However, conventional auditing procedures, e.g. inquiry, recalculation, inspection will still be used.

2.2 Opening balance

* inspect prior year workpapers and prior year financial statements to confirm that the opening balance agrees with the prior year closing balance.

2.3 Occurrence/existence

* inspect the Memorandum of Incorporation to determine whether
  - the company is authorised to issue debentures
  - the issue has in any way contravened the company's borrowing powers, e.g. authority requirements
  - inspect the minutes of the meeting of directors at which the decision to issue debentures was taken and note
    - to whom the issue was to be made
    - the number and amount of the debentures to be issued
    - the interest rate, date and manner of payment
    - any particular characteristic of the debenture e.g. repayable at a premium, convertible to shares.

Note: the directors do not need shareholder approval to issue debentures, except where the directors intend to issue debentures convertible into shares, to themselves. If this is the case, Companies Act Sec 41 will apply (basically special resolution from shareholders unless exceptions apply).

* inspect the register of debenture holders to confirm that the addition of new debenture holders and adjustments to the holdings of existing debenture holders, have been made according to the authority granted for the issue.
* inspect the cash receipts journal, deposit slip/bank statements for evidence of the receipt of the correct amount.

2.4 Accuracy, cut-off, classification

2.4.1 initial recognition (on issue)

* reperform the calculations and casts to confirm that the cash received from the issue of the debentures is in accordance with the debenture agreement e.g. 100 debentures of R1 000 = R100 000 received (accuracy)
* trace the receipt of cash from the cash receipts journal to the general ledger to confirm that it was posted to the debenture liability account (classification)
* inspect the dates on all documentation to confirm that they fall within the accounting period under audit (cut-off).

2.4.2 Subsequent measurement

* recalculate the effective interest rate based on the terms of the debenture agreement and compare to the effective interest rate used by the client in the amortisation calculation
* inspect the journal entry raising the finance cost and increasing the debenture liability account and agree the amounts to the amortisation calculation.

2.5 Completeness

* confirm by inquiry of the directors and scrutiny of the minutes that no other debenture issues have taken place during the year.

2.6 Closing balance

* agree the closing balance on the debenture account (after the finance charge/amortisation adjustment) to the trial balance.

2.7 Assertions pertaining to presentation and disclosure

* The auditor must inspect the disclosures made and consider whether
  - they are complete in terms of the applicable accounting framework, e.g.
    - details of any security which has been granted to debenture holders – e.g.

a bond over fixed property
- dates and conditions of any redemptions or conversion options

- they are consistent with evidence gathered on the audit
- amounts, facts, details etc are accurate and agree with the evidence obtained
- any classification of the information disclosed is appropriate
- the wording of disclosures is clear and understandable.

2.8 General

* if necessary, obtain a 3rd party confirmation from the debenture holders (confirm amount of debenture, interest rates, redemption premium and conditions of redemption). This relates to all assertions.

3. LONG-TERM LOANS

Borrowing long term is a common form of financing. The audit plan will be to audit substantively the opening balance, movement on the account including any adjusting journal entries, and the closing balance. Ultimately the auditor seeks evidence about the assertions relating to the balance on the long-term liabilities account i.e. ***obligation, existence, valuation, completeness*** as well as evidence to support the assertions applicable to presentation and disclosure of information about this account heading**.** This is achieved by auditing the transactions making up the account for ***accuracy, cut-off, classification, completeness*** and ***occurrence*** and supplementing these with procedures relating to the final balance. Generally speaking the dominant risk is ***completeness*** so the auditor will be concerned about any long-term loans ***not*** recorded.

3.1 Important accounting aspects – Long term loans

Long term loans should be reflected at amortised cost using the effective interest rate. For a normal long term loan e.g. fixed term, no premium on repayment etc, the effective interest rate will be the annual interest rate charged per the agreement. There may be a situation where the company raises a long term loan which has a low annual interest rate (to assist with cash flow) but which must be repaid, at the end of the loan term, at a premium. Such a loan would have to be amortised at the effective interest rate to spread the full cost of the loan over the term of the loan (very similar to a debenture redeemable at a premium).

3.2 As the audit procedures are so similar to those for debentures as discussed above, they have not been repeated here. However, additional procedures pertaining to the ***completeness*** assertion have been included below as this is an assertion for which there is potential for material misstatement i.e. understatement of liabilities.

3.3 Completeness of long term loans procedures

* obtain specific representations from management that all long-term loans have been included.
* review financial records, minutes of directors, audit committee and capital expenditure committee meetings and correspondence for evidence of unrecorded loans.
* obtain 3rd party confirmations from all long term loan creditors from the prior year, who are no longer reflected as long-term liabilities, or whose balances are significantly lower in the current year.
* enquire and confirm as to the source of funding for any major acquisitions identified during the audit of non-current assets.
* match interest payments to long-term loans to confirm the loan to which the interest payment relates has been raised.
* perform analytical review e.g. compare current year balances on loan accounts and interest paid to the prior year.

4. FINANCE LEASE LIABILITIES

Leasing is another very common form of "acquiring" an asset. Many leases are simple operating leases for which the lease rentals paid are expensed through profit and loss. However, finance leases are

treated very differently and require that the company raise an asset and a corresponding liability. The audit of a finance lease is therefore far more difficult and requires that both the asset raised and the corresponding liability be audited. The assertions which pertain to assets and liabilities as well as to transactions all apply, sometimes overlapping with each other.

4.1 Important accounting aspects - Finance lease liabilities

* The auditor must be aware of the guidance contained in IAS 17 – Leases. With regard to leases, a lease is classified as a finance lease, and hence must be capitalized, if individually or in a combination, the following conditions are present:
  - that the lease agreement transfers ownership of the asset to the lessee at the end of the lease term, or
  - the lessee has the option to purchase the asset at a price that is expected to be sufficiently lower than the fair value at the date the option becomes exercisable for it to be reasonably certain, at the inception of the lease, that the option will be exercised (bargain purchase option)
  - the lease term is for the major part of the leased asset's economic life, or
  - the present value of the minimum lease payments (at the inception of the lease) amounts to at least, substantially all of the fair value of the leased asset
  - the leased assets are of a specialised nature such that only the lessee can use them without major modification.

  Further indicators include
  - if the lessee cancels the lease, the lessor's losses associated with the cancellation are borne by the lessee
  - gains or losses from the fluctuation in the fair value of the residual value accruing to the lessee, and
  - the lessee has the ability to continue the lease at a rent that is substantially lower than the market rent.

* where a lease is to be capitalized as a finance lease, an asset and corresponding liability must be recognised in the statement of financial position. Essentially this gives rise to four requirements.

  Requirement 1
  - the asset must be raised at its fair value or, if lower, the present value of the minimum lease payments discounted at the interest rate implicit in the lease agreement
  - any direct lease costs incurred by the lessee may also be capitalized.

  Requirement 2
  - the asset must, like any other fixed asset, be appropriately depreciated (IAS 16)
  - if it is not reasonably certain that ownership will transfer to the lessee, the asset will be depreciated over the ***shorter*** of the lease term or its useful life
  - if there is reasonable certainty that ownership will transfer to the lessee, the asset is depreciated over its useful life.

  Requirement 3
  - as the lease payments are made, the payment must be apportioned between finance charges and the reduction of the liability.

  Requirement 4
  - the current portion of the lease liability must be disclosed under current liabilities.

4.2 Occurrence/ obligation and existence

* inspect the finance lease agreements for pertinent details:
  - name of lessor and lessee (i.e. client)
  - amount of minimum lease payments
  - term of lease
  - other salient conditions e.g. penalties for late payment of lease rental .

* inspect the minutes of directors and capital expenditure committee's meetings authorising the lease agreement.
* inspect the Memorandum of Incorporation to confirm that they have been complied with, in particular that the borrowing powers/conditions have not been breached.
* enquire of management and refer to prior working papers, to confirm that new finance will not breach contracts in respect of existing finance arrangements.
* determine whether the lease qualifies as a finance lease i.e. the risks and rewards of ownership have substantially transferred to the lessee (see important aspects).

4.3 Completeness

* obtain specific representations from management that all finance leases have been included.
* review financial records, minutes of directors, audit committee and capital expenditure committee meetings and correspondence for evidence of unrecorded liabilities e.g. use of leases to provide "off-balance sheet finance", when in fact they should be classified and treated as finance leases.
* enquire and confirm as to the source of funding for any major acquisitions identified during the audit of fixed assets.
* obtain a schedule of all leased assets and by inspection and enquiry, determine whether any leases that have been classified as ***operating,*** should be finance leases.
* obtain a schedule of ***all*** lease payments, and match to lease agreements to confirm that all leases have been identified. Confirm by scrutiny of the agreements that all finance leases have been identified and capitalized.
* perform analytical procedures e.g. compare current year balances on finance lease accounts and lease payments paid to the prior year.

4.4 Accuracy, cut-off, classification

4.4.1 Initial recognition

* obtain independent confirmation of the fair value of the asset which has been leased by enquiry of the supplier, inspection of trade journals etc. (the fair value is unlikely to appear in the lease agreement).
* if any direct lease costs have been capitalized, confirm by enquiry and inspection of the supporting documentation that the costs are valid lease costs applicable to the leased asset and were incurred by the lessee.

4.4.2 Depreciation – leased asset

* by enquiry of management and evaluation of the terms of the lease agreement, determine whether the asset should be depreciated over its useful life or the term of the lease.
* determine by enquiry of the directors whether the residual value applicable to the leased asset, is reasonable .
* determine by enquiry of the directors whether the "significant part" method of depreciation is applicable and if so, whether the allocation of costs of the components is appropriate (independent enquiry of the supplier may be required).
* enquire of the directors as to whether the depreciation method e.g. straight line, units produced, is appropriate, and confirm by reference to the minutes that the method has been reviewed by the directors (must be done annually).
* reperform the depreciation calculation.
* enquire of production director as to whether any impairment of the asset is required.

4.4.3 Lease payments

* reperform the implicit interest rate calculation.
* reperform the apportionment calculation of the leased payments and trace the posting of the amounts apportioned to the liability account (and finance cost account).
* reperform the "current portion of the lease liability calculation**"** and trace the reclassification to the general ledger/trial balance/financial statements.

4.4.4 General

* cast the finance lease liability account.
* by scrutiny of dates on documentation confirm that the leases, repayments etc relate to the accounting period under audit.

4.5 Assertions pertaining to presentation and disclosure

* The auditor must inspect the disclosures made and consider whether
  - they are complete in terms of applicable accounting framework, e.g.
    - accounting policies
    - amounts and commitments
    - terms of leases
    - encumbrances on any leased assets
    - reconciliation between the total of future minimum lease payments at reporting date, and their present value
  - they are consistent with evidence gained on the audit
  - amounts, facts, dates etc are accurate and agree with the evidence gathered
  - any classification of the information disclosed is appropriate
  - the wording of disclosures is clear and understandable.

Note: The disclosures pertaining to non-current liabilities are extensive, and it is very likely that the auditor will be required to carry out extensive procedures ***specifically*** pertaining to disclosure, i.e. procedures in addition to those conducted when auditing the "transaction and balance" assertions.

5. PROVISIONS, CONTINGENT LIABILITIES AND CONTINGENT ASSETS

To achieve fair presentation, companies are obliged to make adjustments for certain anticipated events or to disclose them. The former is termed a provision and the latter is termed a contingent liability/asset.

In common accounting language the term "provision" is frequently used in connection with bad debts, inventory obsolescence and depreciation, e.g. provision for bad debts. This is not theoretically the correct terminology as these "provisions" do not fit the provision definition in IAS 37. The term that is being used more and more is "allowance" e.g. allowance for bad debts or impairment allowance for accounts receivable, or allowance for inventory obsolescence. Situations which might give rise to provisions (should the definition be satisfied) include

* a provision for the cleaning up of environmental damage caused by the company
* a provision for refunds to dissatisfied customers
* a provision for damages arising out of a courtcase.

Contingent liabilities are similar to provisions but not as "certain". Provisions and contingent liabilities (and contingent gains) are, however, treated differently in the financial statements. Provisions are recognised as liabilities provided the amount can be measured with sufficient reliability. They are included in the statement of financial position whereas contingent liabilities are only disclosed in the notes.

5.1 Important accounting aspects

* ***Definitions*** (IAS 37)
  - ***provision*** — a liability of uncertain timing or amount
  - ***liability*** — a ***present*** obligation of an entity arising from past events, the settlement of which is expected to result in an outflow of resources from the entity
  - ***contingent liability*** — a ***possible*** obligation that arises from past events, and the existence of which will be confirmed only by the occurrence or non-occurrence of an uncertain future event not wholly in the control of the entity.

* ***Recognition of provisions and contingent liabilities***

- ***provisions*** - a provision must be recognised when
  - the company has a ***present obligation*** as a result of a past event
  - it is ***probable*** that an outflow of resources will be required to settle the obligation
  - a reliable estimate can be made of the amount of the obligation.

If these conditions are not met, no provision shall be recognised ***but*** the matter will still be disclosed in the notes as a contingent liability.

- ***contingent liabilities*** – contingent liabilities are not recognised but must be disclosed.

* ***Contingent assets***

A contingent asset is a possible asset that arises from past events and whose existence will only be confirmed by the occurrence or non-occurrence of an uncertain future event not wholly within the control of the entity, e.g. successful outcome of a courtcase where the company is awarded damages.

Contingent assets are not recognised in the financial statements but, where the inflow of economic benefit is probable, are disclosed. If the economic benefit is "virtually certain" the asset is not regarded as "contingent" and should be recognised. The auditor should satisfy himself on the basis of all the evidence available whether a contingent asset exists at reporting date, and whether the economic inflow is probable (disclosure) or virtually certain (recognition).

* ***Commitments***

Companies are also required to make disclosures pertaining to "commitments". To identify any commitments which should be disclosed the auditor will perform very similar procedures to those conducted for provisions and contingent liabilities, e.g. enquiry of the directors and scrutiny of the minutes of directors' meetings may reveal commitments for capital expenditure, contracted and approved, which must be disclosed. The assertions applicable to presentation and disclosure will apply to commitments.

5.2 Implications for the auditor

As indicated earlier the provisions and contingent liabilities that are being discussed here are not as straightforward as the normal allowances for bad debts, inventory obsolescence etc. They may be varied in nature and may be unique to particular industries.

Provisions are recognised and therefore there will be a "provisions" account in the general ledger, the assertions applicable to which will be:

completeness - all provisions have been included in the account balance
existence - the provisions included are not fictitious
valuation - the provisions are included at an appropriate amount
obligation - the provisions represent an obligation of the entity.

In addition the auditor must satisfy himself that the provisions are appropriately presented and described in the financial statements and that related disclosures in the notes are clearly expressed, accurate and understandable.

Contingent liabilities are not recognised but are disclosed in the notes. The applicable assertions relating to this disclosure are:

Completeness - all contingent liabilities have been included in the notes
Obligation - the contingent liabilities disclosed pertain to the entity
Occurrence - the event giving rise to the contingent liability has actually occurred (it is not fictitious)
Understandability - the disclosures pertaining to the contingent liabilities are appropriately described and clearly expressed
valuation and accuracy - information provided in the disclosure is fair and accurate and values included are appropriate.

5.3 Audit procedures – provisions and contingent liabilities

The audit procedures for provisions and contingent liabilities are very similar as they are, themselves, very similar in nature.

5.4 Existence

Under normal circumstances a company will not wish to include provisions and contingent liabilities which are fictitious. However, there is the possibility that provisions that do not meet the definition criteria are included in the account heading, or that the directors wish to manipulate the financial statements by the inclusion of fictitious provisions or contingent liabilities. Procedures to test the existence of provisions and contingent liabilities are as follows:

* evaluate the company's procedures for identifying provisions and contingent liabilities.
* inspect the supporting documentation which management provides for each provision recognised and
  - evaluate whether there is a legal or constructive present obligation arising out of a past event which actually occurred
  - evaluate the probability that an outflow of resources will be required to settle the obligation
  - evaluate the basis on which the amount of the obligation was determined to decide whether a reliable estimate could be made
* inspect the documentation which management supplies in support of contingent liabilities disclosed and evaluate whether there is a possible obligation whose existence will only be confirmed by the occurrence or non-occurrence of an uncertain future event.
* consider the process used to authorise the recognition/disclosure of provisions and contingent liabilities (authority minuted by the Board may reduce the risk of invalid provisions).
* discuss any uncertainties or concerns arising out of the above evaluations with the directors.
* if necessary seek legal counsel, or the advice of an expert (e.g. in industry specific matters such as provisions for environmental damage).

5.5 Valuation

The value at which the provision is recognised is the "reliable estimate of the amount of the obligation". The auditor is thus auditing an estimate. ISA 540 – Auditing accounting estimates, including fair value accounting estimates and related disclosures, provides guidance. The auditor should assess the risk of material misstatement of the entity's accounting estimates (in the normal manner) and design and perform further audit procedures to obtain sufficient appropriate evidence as to whether the accounting estimates are reasonable in the circumstances and, where necessary appropriately disclosed.

The statement requires that

* the auditor identify and assess the risk of material misstatement of accounting estimates.
* when performing risk assessment procedures (at the understanding the entity phase), the auditor should obtain an understanding of:
  - the requirements of the applicable accounting framework relevant to accounting estimates (e.g. IFRS/IAS 37)
  - how management identifies transactions, events and conditions which may give rise to the need for accounting estimates
  - how management makes the estimate e.g. use of a model, use of an expert, the assumptions underlying the estimate and the effect of estimation uncertainty (this is defined as "the susceptibility of an accounting estimate and related disclosures to an inherent lack of precision in its measurement").
* the auditor review the outcome of prior year accounting estimates (in effect this provides information as to the effectiveness of the company's estimate setting procedures).

The auditor should

* review and test the process used by management to develop the estimate including the approval/authorisation procedure (internal controls over the procedure).
* evaluate the data on which the estimate is based for accuracy, completeness and relevance
* evaluate the reasonableness and consistency of any assumptions which have been used in developing the estimate
  - reasonable in the light of actual prior performance

- consistent with the assumptions used for other similar estimates.

* reperform any calculations pertaining to the estimate.
* compare the amount of the estimate to similar estimates.
* compare the amount of the estimate made in prior periods with actual results for that period i.e. estimates of warrantee claims compared to actual warrantee claims.

The auditor may also make his own estimate or obtain an independent estimate from an expert. In this case any differences with the client's estimate should be discussed with management and resolved if possible.

The value at which the contingent liability is disclosed would have to be evaluated by reference to the supporting documentation and enquiry of management supplemented by evidence gained when conducting the procedures above.

5.6 Obligation

As with the existence assertion, under normal circumstances it is unlikely that the company will include provisions or contingent liabilities that are not obligations of the company itself. If the auditor considers that there is a risk of this occurring, he would need to satisfy himself, by enquiry of the directors, experts or legal counsel, and inspection of the supporting documentation, that the provisions recognised are obligations of the company, not the directors, related parties or anyone else.

5.7 Completeness

As indicated earlier, this assertion probably represents the most significant risk for the auditor – the risk that the company will understate/omit provisions either intentionally or unintentionally. Material intentional understatement by the directors would amount to fraudulent financial reporting (as would material overstatement, but this is generally a lesser risk) and may be very difficult to uncover. The following procedures should be carried out:

* evaluate the company's processes and procedures for identifying the need for provisions.
* compare the schedule of provisions for the current year to that of the prior year and follow up on any which are not included on the current year's list or which have reduced significantly.
* compare the contingent liabilities currently disclosed to those disclosed at the prior year-end and follow up on the status of contingent liabilities disclosed at the prior year-end.
* enquire of the company's legal advisers as to whether the company is involved in any disputes/defending any legal action and request them to provide details of the probable or possible losses arising from such actions and also of the legal costs involved.
* inspect the minutes of directors and shareholders meetings for evidence of the need for provisions e.g.
  - warrantee claims
  - guarantees
  - environmental damage
  - refund policies
  - closure of a division of the company.
* inspect correspondence, returns etc relating to taxation matters/SARS.
* inspect the cash payment records subsequent to year-end for unusual material payments and follow up to determine whether they are in respect of an obligation which should have been provided for at year-end.
* obtain a confirmation certificate from the company's bankers detailing
  - guarantees for loans
  - discounted bills etc.
* discuss the completeness of the provisions with management and request specific reference to completeness of provisions in the management representation letter.

5.8 Assertions pertaining to presentation and disclosure

* The auditor must inspect the disclosures made and consider whether

- they are complete in terms of the applicable accounting framework e.g.
  - carrying amounts of provisions at the beginning and end of the period
  - additional provisions made and increases to existing provisions
  - unused amounts reversed
  - a brief description of the nature of the obligation and the expected timing of any resulting outflows
  - a brief description of each contingent liability and an estimate of its financial effect.
- they are consistent with evidence gained on the audit
- amounts, facts, details etc are accurate and agree with the evidence gathered
- any classification of the information disclosed is appropriate
- the wording of the disclosures is clear and understandable.

Note: The list of disclosure requirements given above is not complete, reference should be made to IAS 37.

AUDIT PROCEDURES - THE INVESTMENT CYCLE

1. PROPERTY, PLANT AND EQUIPMENT

In terms of IAS 16 "Property, Plant and Equipment", assets falling into this category include:

* land and buildings,
* plant and machinery,
* vehicles, and
* furniture and equipment.

The audit procedures for each of these categories are very similar and therefore will be described collectively, rather than individually. The assertions pertaining to the balance of the PPE accounts, which the auditor is concerned about, are ***existence, completeness, rights and valuation***. In addition the auditor must consider the assertions relating to the presentation and disclosure of property, plant and equipment.

Remember that when the movement (additions and disposals) on the account is audited, you will be auditing the assertions relating to transactions, primarily ***occurrence*** and ***accuracy, classification and cut-off***. Procedures for auditing the carrying value of the asset will include procedures relating to the depreciation allowance and any impairments. Most clients will present the auditor with schedules for the asset accounts and related accumulated depreciation accounts, which reflect:

Cost :

Opening balance	Additions	disposals	closing balance
R1 641 900	4 21 816	243 804	1 819 912

Accumulated depreciation and impairments :

Opening balance	Provision/impairment	disposals	closing balance
R542 813	274 601	113 816	703 598

The example contains only totals. Each column will be broken down into the individual assets making up the total. For example, the "additions" column may be made up of the cost price of six new assets, and the "disposal" column may be made up of the cost of three assets disposed of.

The schedules may also contain columns which deal with adjustments e.g. revaluations.

The auditor's task is essentially to audit these schedules. Companies are also obliged to keep fixed asset registers which are very useful to the auditor when gathering evidence about fixed assets.

1.1. Important accounting aspects : Property, plant and equipment

IAS 16 – Property, Plant and Equipment, governs the accounting treatment of property, plant and equipment.

The auditor should be aware that IAS 16 offers two possible methods of valuing PPE, the cost model and the revaluation model. As per IAS 16, the model chosen must apply to the entire class of PPE, e.g. the company cannot decide to use the cost model for some of its machinery but not for other pieces of machinery. The company may however, use the cost model for machinery and the revaluation model for land.

1.2 Cost model

After recognition as an asset, an item of PPE must be carried at its cost, less any accumulated depreciation and any accumulated impairment losses.

The cost of an item of PPE normally comprises

* its purchase price including import duties etc
* costs directly attributable to bringing the asset to the location and condition necessary for it to operate in the intended manner, e.g. cost of site preparation, cost of employee benefits relating directly to the production or acquisition of the item, installation and assembly costs, related professional fees, e.g. engineers.

1.3 Revaluation model

After recognition as an asset, an item of PPE, whose fair value can be measured reliably, shall be carried at a revalued amount, being its fair value at the date of the revaluation, less any subsequent accumulated depreciation or subsequent accumulated impairment losses. Revaluation must be made with sufficient regularity, so as to ensure that the carrying amount does not differ materially from that which would be determined using fair value at reporting date.

1.4 Depreciation

IAS 16 requires that "each ***part*** of an item of property, plant and equipment with a cost that is significant in relation to the total cost of the item shall be depreciated separately". Expressed differently this means that the directors should allocate the cost of the item to its ***significant parts*** and depreciate each part separately. This should happen where:

* the cost of the part is significant in relation to the total cost of the item
* the part and the remainder of the unit have different useful lives or
* different residual values.

For example Ultrasize Ltd, a large manufacturing company, uses a steel press which it originally purchased as one piece of machinery but which consists of two components, namely a hydraulic power press and a steel pressing platform. Both parts of the machine are in themselves very expensive, but the hydraulic power press has a useful life of 10 years, whilst the pressing platform will last for 30 years. Total cost of the machine is R10 million with the press as a separate unit costing R4 million and the platform R6 million. Instead of depreciating the steel press as a single item, the two components are depreciated separately.

Note that if the points above apply, the "significant parts" policy must be applied. There are difficulties however. For example, how is the residual value of each significant part established, particularly if there is no market in which to sell the significant part? Should the company use a residual value of nil? Can the useful life of the "significant part" and the remainder, be separately determined?

From a practical point of view this kind of problem is only likely to occur in large companies with huge investments in PPE. However, this does have implications for the audit, as the auditors are required to assess whether IAS 16 has been applied and that it has been applied correctly.

Where the item has been broken down into significant parts, each part will be recorded in the fixed asset register separately.

IAS 16 states that the depreciable amount of an asset shall be allocated on a systematic basis, over its useful life. IAS 16 provides the following definitions:

* ***depreciable amount*** is the cost/revalued amount, less the residual value

* ***residual value*** of an asset is the estimated amount that an entity would currently obtain from the disposal of the asset, after deducting the estimated costs of disposal, if the asset were already of the age and in the condition expected at the end of its useful life

* ***useful life***:
  - the period over which an asset is expected to be available for use by an entity, or
  - the number of units expected to be obtained from the use of the asset, by the entity.

IAS 16 requires that the depreciation method used must reflect the pattern in which the assets future economic benefits are expected to be consumed, e.g. straight line method, diminishing balance, unit of production method.

IAS 16 states that the residual value and useful life shall be reviewed at least at the end of each financial year-end, and if expectations differ, changes should be accounted for, as per IAS 8 – Accounting Policies, Changes in estimates and Errors.

1.5 Audit procedures – property, plant and equipment

1.5.1 Existence

* extract a sample of assets from the fixed asset register, which includes (all or some) additions for the year. If the client's fixed asset register is computerised, audit software can perform this task.
* physically inspect the assets selected, matching them to the description (e.g. serial numbers) obtained from the fixed asset register.
* if an asset cannot be physically verified for existence e.g. it is a large piece of mobile equipment being used in a remote area, seek corroborating evidence e.g. drivers' wages, licence, correspondence with customer, repairs and maintenance records.
* conduct a search of ***unrecorded*** disposals (mainly for plant and equipment)
  - analyse the sundry revenue account/cash receipts journal for cash receipts from disposals of fixed assets; confirm that the item for which the cash has been received, is included on the list of disposals.
  - during physical inspection of assets, take note of any evidence of "fixed" equipment which has obviously been removed and follow up to determine whether a disposal has taken place and is recorded.
  - enquire of senior personnel (factory manager) whether major equipment acquired has replaced old equipment; if so, follow up to determine whether old equipment was disposed of and recorded as a disposal.
  - inspect correspondence with insurance company to identify any fixed assets, which have been removed from the list of insured items. Follow up to determine whether such items have been disposed of and if so, that they appear on the list of disposals.
  - look for evidence of expenses related to property, plant and equipment which are no longer being paid or are significantly reduced, e.g. a vehicle licence, rates on a property, significant decline in motor vehicle costs. Confirm that the asset to which the expense relates, has been treated as a disposal if it no longer "exists".
* reconcile disposals per the capital budget with client's list of disposals.

1.5.2 Completeness

* inspect repairs and maintenance and similar accounts for material items which may represent acquisitions of plant and equipment, but which may have been erroneously charged as an expense.
* when physically verifying the assets for existence, select a sample of fixed assets and trace to the fixed asset register agreeing description, asset number etc.
* review payments for fixed asset purchases and confirm that they are recorded as fixed assets in the register.
* review all lease agreements and enquire of senior personnel for evidence of any assets, which have been leased in terms of finance leases, but which have not been capitalised.

1.5.3 Rights

* for assets owned at the beginning of the financial year (opening balance), determine whether there has been any change in the rights to the asset, e.g. sale and leaseback, by
  - enquiry of management
  - inspection of directors' minutes.
* for additions, inspect purchase documentation and documents of title, to confirm that they are in the name of the client:
  - for motor vehicles, inspect the ***registration document*** and ***licence renewal receipt*** to confirm that they are in the name of the client.
  - for land, inspect the title deeds/deeds of transfer, mortgage bonds and sale agreements.
  - for other assets, inspect sales agreements and invoices.
* where assets are still being paid for, confirm that the client is not behind with payments, (thus jeopardising rights), by inspection of payment records and supplier statements and enquiry of the financial manager (if appropriate the supplier can be contacted).
* where leased assets have been capitalised, inspect the lease agreements to ensure that the risks and rewards of ownership have effectively passed to your client. See Important Accounting Aspects – Finance Lease Liabilities.
* by enquiry of management and inspection of
  - prior year working papers
  - minutes
  - loan agreements
  - bank and other 3rd party confirmations

  obtain evidence of any encumbrances on fixed assets e.g. offered as security.

1.5.4 Valuation – cost

* agree the opening balances on the summary schedules to prior year work papers/general ledger.
* reperform all casts and extentions in the fixed asset register, the summary schedules and the supporting lists of additions and disposals.
* reperform the reconciliation of the fixed asset register to the fixed asset accounts and accumulated depreciation accounts in the general ledger, following up on all reconciling items.
* agree by inspection, the closing balances on the summary schedules to the general ledger and financial statements.

1.5.5 Cost of additions

occurrence

* select a sample of additions from the fixed asset register and trace to capital budget, minutes of directors' meetings and purchase requisitions for evidence of authority for the acquisition.
* inspect the asset itself and cross reference description, serial number, etc to purchase documentation.
* inspect the purchase documentation (invoice, contract) to confirm that it is made out to the client, is for the selected fixed asset and is signed.
* inspect payment records to confirm that payment was made for the asset.

accuracy, classification, cut-off

* by inspection of the purchase documentation, confirm that the cost of the asset includes:
  - the correct cost price
  - correct shipping charges, import duties, insurance (if applicable)
  - costs of installation and commissioning of the fixed asset (if applicable)
* if the asset is imported, by reperformance, confirm that:
  - it has been raised in the company's records at the spot rate on transaction date.
  - all relevant shipping costs, import charges have been included in the cost and, where appropriate, converted from the foreign currency at the correct rate (transaction date).
* where the company has allocated the total to "significant parts" of the item of PPE, confirm that the allocation is fair by enquiry of the directors and inspection of relevant documentation, e.g. from supplier.
* if the asset has been installed, obtain a schedule of installation costs and:
  - agree it to the cost calculation for the asset
  - inspect the supporting documentation in respect of materials and wages used in installation for valid, accurate and complete inclusion, particularly that there is no inclusion of non-relevant expenses, e.g. repairs.
  - discuss the reasonableness of any other expenses included, with the financial director, e.g. any allocation of overheads.
* by inspection of purchase documentation and the relevant ledger account, ensure that VAT has not been included in the cost (unless client is not a vendor).
* inspect the dates on all documentation e.g. invoice, to confirm that the transaction has been recorded in the correct accounting period (cut-off).
* trace the postings from source to the general ledger to confirm that the transaction has been recorded in the proper accounts (classification).

1.5.6 Disposals

occurrence

* inspect the supporting documentation used to approve the disposal for an authorising signature.
* by reference to the capital budget, confirm authority for the disposal.
* trace the proceeds of the sale to the receipts records/bank stamped deposit slip/bank statement.

accuracy, classification, cut-off

* obtain the original cost/revalued cost of the asset disposed of, dates of acquisition and disposal, from the fixed asset register and
  - recalculate accumulated depreciation to date of disposal
  - recalculate the profit/loss on sale*
  - inspect the dates on all documentation to confirm that the disposal has been recorded in the correct accounting period (cut-off)
  - confirm by inspection that the asset account and accumulated depreciation accounts in the general ledger have been correctly amended and that the disposal has been correctly and completely recorded in the fixed asset register (accuracy and classification).

*Note: If a fixed asset is sold at an amount below its carrying value, its selling price may have been arrived at as a result of an impairment assessment. If so, in theory the asset should be written down to reflect the impairment. This means that there would not be a loss on sale but rather an impairment loss. If the asset is sold without an impairment assessment, the loss would be recorded as a loss on sale.

1.5.7 Valuation – depreciation allowance

* confirm by enquiry of the directors that the accounting policy for depreciation is consistent with prior years.
* where the "component" (significant part) method of depreciation has been adopted, confirm that the allocation total of cost to the components is fair and reasonable by
  - enquiry of management

- scrutiny of purchase documentation or
- enquiry of the supplier.

* obtain a representation letter from management, confirming that they have reassessed the useful life and residual value of the assets (as required by IAS 16) including those of separate "components" where applicable.
* review the changes (if any) to the useful life and residual values, and assess the reasonableness of the changes. Obtain reasons from management and, if necessary, consult an expert with regard to the residual value/useful life.
* when physically inspecting fixed assets inspect for, and enquire about, any damaged or "not in use" assets and establish whether such items should be written down.
* extract a sample of assets, which were acquired (say) 4 years previously and compare their physical condition to their depreciated value.
* by inspection and analysis of any profits/losses on disposals of fixed assets, consider whether the depreciation method is reasonable, i.e. estimates of useful life and residual value are appropriate.
* reperform the depreciation calculations for the year to ensure accuracy and compliance with the depreciation policy, and that amounts have been correctly posted.
* discuss the reasonableness of the depreciation allowance with management and enquire into the approval procedures adopted, e.g. does the financial director review the allowance.
* perform analytical procedures on the allowance, e.g. comparing to prior years, by asset grouping, and in relation to the additions and disposals for the year.
* discuss with senior personnel e.g. factory manager, whether there has been anything which may affect useful life e.g. machinery running on double shift for the first time.

1.5.8 Valuation- impairment

In terms of IAS 36 – Impairment of Assets, a company must assess at each reporting date whether there is any indication that an asset may be impaired. If any such indication exists, the entity shall estimate the recoverable amount of the asset so that any impairment loss can be calculated. An impairment loss is the amount by which the carrying amount of an asset exceeds its recoverable amount (i.e. an asset will be impaired if the amount which could be recovered through the use or sale of the asset, is exceeded by its carrying value). The auditor will probably be largely dependent on the directors to identify and quantify the impairment and there may well be a fair amount of subjectivity involved. The auditor should do at least the following:

* evaluate the process by which the company itself identifies and quantifies impairments.
* inspect and evaluate any documentation which might support the directors on impairments with regard to
  - assumptions made
  - methods or bases of quantification
  - rates or percentages used.
* discuss with management
  - any assets whose market value has declined significantly more than would be expected as a result of the passage of time or normal use
  - any significant changes which might have taken or might be about to take place, which would adversely affect the entity in the technological market, economic or legal environments in which the company operates
  - any evidence obtained on the obsolescence or physical damage to assets identified during the audit
  - assets lying idle, plans to discontinue certain operations etc
  - evidence from internal reports, e.g. monthly management reports that suggest that economic performance of an asset is worse than expected.

1.5.9 Revaluations

A company can choose the ***cost model*** (i.e. the asset is carried at its cost, less any accumulated depreciation and any accumulated impairment losses) or the ***revaluation model*** (i.e. any item of property, plant and equipment whose fair value can be measured reliably) shall be carried at a revalued amount, being its fair value (the amount for which an asset could be exchanged between knowledgable willing parties in an arms length transaction) at the date of the revaluation, less any

subsequent accumulated depreciation and impairment losses. Although the audit procedures relating to the substantive testing of Property, Plant and Equipment will basically be the same, the choice of the revaluation model will have some implications for the auditor.

Frequently, particularly with Land and Buildings, the revaluation is determined from market based evidence evaluated by an expert e.g. a property valuator. Where this is the case, the auditor will follow the guidance given in ISA 620 – Using the work of an Auditor's Expert, which is covered in Chapter 16, to assist in the audit of the revaluation.

For other classes of PPE there may be reliable external sources to which the auditor can refer to gather evidence about fair value of the asset. For example, there are numerous sources which provide the fair value of used motor vehicles and heavy equipment such as front end loaders etc.

Where the revaluation has been carried out internally (e.g. by the directors), the auditor would have to audit the supporting documentation to evaluate the reasonableness of the methods used, the assumptions made and the interpretations by the directors of any available data. Of course the auditor would need to verify data used whenever possible.

In addition to the above, the auditor would pay careful attention to the treatment of accumulated depreciation at the date of revaluation and subsequent thereto. All calculations would be checked as would the treatment in the financial statements of any increases or decreases in the carrying value. If the asset's carrying value increases, the increase would first be recognized in profit or loss (as a credit to income) to the extent that it reverses a previous decrease that was recognized in profit or loss. Any increase that does not reverse a previous decrease recognized in profit or loss is recognized in other comprehensive income (as a credit to revaluation surplus). If the asset's carrying value is decreased, this decrease must first be debited to the revaluation surplus account (if any) before being expensed as a revaluation expense in profit or loss.

The auditor would also confirm that ***all*** items in the class of assets (not only particular ones) had been revalued, and that details of the revaluations had been properly disclosed.

1.5.10 Assertions pertaining to presentation and disclosure

To satisfy himself as to the assertions relating to the presentation and disclosure the auditor must inspect the disclosures made and consider whether

* they are complete in terms of the applicable accounting framework, e.g.
    - the measurement bases used for determining the gross carrying amount of each class of property, plant and equipment
    - depreciation methods used
    - a reconciliation of the carrying amount at the beginning and end of the period showing additions, revaluations, impairments, depreciation
    - restrictions on title, capital commitments
    - amounts of impairment losses recognised in profit and loss during the period.
* they are consistent with evidence gained on the audit.
* the amounts, facts, dates etc are accurate and agree with evidence obtained.
* any classification of the information disclosed is appropriate.
* the wording of the disclosures is clear and understandable.

Note: The disclosures applicable to Property, Plant and Equipment are comprehensive and it is very likely that the auditor will be required to carry out procedures ***specifically*** pertaining to disclosure i.e. procedures in addition to those conducted when auditing the "transaction and balance" assertions.

1.6 The use of audit software (substantive procedures)

If the client's fixed assets are computerised and suitable audit software is available, the auditor should make use of it. The software may be put to the following uses:

* a sample of property, plant and equipment can be selected randomly or after stratification of the population by amount, location or class of asset, for physical verification.

* lists of all additions and disposals can be extracted (using date acquired/disposed fields) to be compared with client summary lists. Samples can be extracted for transaction vouching.

* the entire fixed asset masterfile (asset register) can be scanned for "error" conditions:
  - missing or duplicated assets if asset numbers are sequenced
  - blank fields e.g. no asset number, no description
  - anomalies e.g. current depreciation exceeds accumulated depreciation or cost (none should be found)
  - negative book value (none should be found).

* all casts and calculations can be recomputed and compared to client calculations for accuracy e.g. depreciation calculations, net book value calculations.

* the masterfile can be extensively sorted and summarised for analytical procedures, depending upon the fields which are available on the masterfile e.g. asset class, location, current depreciation by class etc. Once sorted and summarised, comparisons can be made to prior years, etc.

Note: The greater the amount of information on the masterfile, the greater the use to which the software can be put. Fixed asset masterfiles will usually contain at least the following, which gives the auditor plenty to work with:

- asset number
- description
- date of purchase
- cost
- depreciation rate and method
- current year depreciation
- accumulated depreciation
- book value
- date of disposal
- disposal price
- impairment details
- revaluation details

2. INVESTMENTS IN SHARES

In today's business environment there are numerous kinds of investments which a company can make, such as bonds, derivatives and the like. The audit of these types of investment is beyond the scope of this text and could almost be regarded as specialist audit knowledge. IAS 32 Financial Instruments – Disclosure and Presentation, and IAS 39 Financial Instruments – Recognition and Measurement, deal extensively with the topic and would be required reading for any auditor whose clients hold such investments.

This section deals with the audit of simple investments of shares in listed and non-listed companies and we have assumed that the audit client ***does not trade*** in shares and investments. The assertions, which the auditor will be concerned with, will be ***rights, existence, valuation*** and ***completeness***. Attention will also be given to the assertions applicable to presentation and disclosure. Again, as it is generally unlikely that there will be numerous transactions, the audit plan will be to audit the opening and closing balances on the account and (a sample of) the transactions (purchase and sale) for ***occurrence*** and ***accuracy, cut-off and classification***.

The major risk will be overstatement of the investment account either by the inclusion of fictitious investments or overstatement of the value of the investment.

As with property, plant and equipment, the client will usually prepare a schedule of investments, reflecting:

* the breakdown between listed and unlisted investments
* details of each investment i.e. name, number and class of shares and percentage holdings
* cost and fair value
* current year movements.

2.1 Rights and existence

* inspect and count the share certificates held by the client, in the presence of a client official, ensuring:

- descriptions, name of company, number of shares, agree to the schedule of investments,
- they are in the name of the client, ***or*** if they are in the name of a nominee, that there are blank transfer forms signed by the nominee to testify to his/her status as nominee in respect of these shares, and
- the share certificates appear to be authentic.

* if listed shares are held and no share certificates are issued (electronic ownership) obtain with client permission, confirmation of ownership direct from the client's brokers.
* if any doubt exists about the existence of a non-listed company in which the client holds shares, contact such company or the Companies and Intellectual Property Commission to establish existence.
* obtain direct confirmation from any bank or other third party, which may hold the client's share certificates as security or in safe custody. This confirmation certificate should:
  - confirm all relevant details on the client schedule, and
  - provide details of the investments pledged as security for the overdrafts or loans.
* ascertain through enquiry and discussion with management that the intention with regard to investments, is to hold them long-term rather than speculate with them. (If the intention is to speculate, the "investment" becomes a trading asset.)

2.2 Valuation – opening balances

* inspect prior year workpapers and financial statements to confirm opening balance agrees with prior year-end balance.

Current year movements

occurrence

* inspect minutes of directors and investment committee meetings for authority to purchase or sell investments.
* inspect brokers notes for evidence of purchase and sale of listed investments, noting descriptions of shares and that brokers notes are addressed to the client.
* inspect contracts and correspondence in respect of purchase or sale of investments in non-listed companies noting description of shares and that contracts are between client and investee and are duly authorised.
*

accuracy, cut-off, classification

* confirm details of cost, selling price and brokerage fees/commissions from brokers notes and sale agreements for both purchases and sales.
* reperform all casts and calculations, particularly where there have been sales, to confirm profit or loss on sale.
* inspect the dates on the documentation to confirm that the transaction has been accounted for in the correct accounting period.
* trace postings to the general ledger from source to confirm that the transaction has been posted to the proper investment account.

2.3 Valuation – closing balance (note in terms of IAS 32, shares in other companies must be valued at "fair value")

* for listed shares, confirm the market value at the financial year-end of the client by inspection of relevant stock exchange publications.
* reperform the client's calculation of number of shares x market price.
* determine by inquiry of the financial director, scrutiny of minutes and/or inspection of the prior year working papers whether the shares have been categorised as financial assets at fair value through profit and loss, or financial assets at fair value through other comprehensive income.
* if the company has elected recognition through other comprehensive income, confirm that the directors have taken and minuted, the decision that the share investment is ***not*** held for trading.
* where there have been gains or losses, confirm by inspection that they have been taken to profit or loss (fair value through profit or loss) or to other comprehensive income (fair

value through other comprehensive income) according to the categorisation adopted by the company and that the treatment is consistent with prior years. (Note: if the company chooses to adopt the other comprehensive income route it is an irrevocable decision.)

* for unlisted investments discuss with the directors, the possibility of obtaining an independent "fair value". Failing this, request that directors provide a "fair value" and assess the reasonableness of their valuation by:
  - inspection of and enquiry about their valuation method and assumptions
  - reperformance of their calculations
  - inspection of latest financial statements of the investee company

  Note: If an independent fair value is provided, the evidence will be audited in terms of ISA 620 – Using the work of an auditor's expert (see chapter 16).

* reperform the casts on the investment schedule, as well as the general ledger accounts and register of investments.

2.4 Completeness

* compare the current year-end schedule to the prior year end schedule and for any decreases in holdings, confirm that there is a disposal recorded under "movement for the year".
* obtain a representation from management in respect of the completeness of investments.
* match any dividends received during the year to the list of investments.
* obtain a summary of dealings in listed shares for the year from the company's brokers.

2.5 Assertions pertaining to presentation and disclosure

The auditor must inspect the disclosures made and consider whether:

* they are complete in terms of the applicable accounting framework, e.g.
  - investments are disclosed on the face of the statement of financial position at "fair value",
  - accounting policies are adequately disclosed particularly how the financial assets are classified and measured and whether gains and losses of financial assets are recognized in profit or loss or in other comprehensive income,
  - dividends (if any) are disclosed separately in the statement of consolidated income, and
  - any encumbrances on investments are fully disclosed.
* they are consistent with evidence gained on the audit.
* amounts, facts and details are accurate and agree with the evidence gathered.
* any classification of the information disclosed is appropriate.
* the wording of disclosures is clear and understandable.

Note: by discussion with the directors and consideration of the percentage holdings, confirm that no investments on the schedule should have been "equity accounted" or "consolidated".

3. LONG-TERM LOANS MADE BY THE COMPANY

Long-term loans made by the company are very similar to debtors and, as expected, the audit procedures will be reasonably similar. The assertions which the auditor is interested in, will be ***rights, existence, valuation, completeness.*** Attention will also have to be paid to the assertions pertaining to presentation and disclosure. The major risk is overstatement brought about by the inclusion of "fictitious" loans, or the failure to write down a loan where repayment is doubtful and security is inadequate. Again any movement on the loan account should be audited as "transactions" e.g. advancing new loans or receiving repayments, in which case ***occurrence*** and ***accuracy, cut-off and classification*** will be the major assertions to be audited. It is again likely that the client will supply a schedule of loans reflecting each loan holder, the opening balance, movements during the year and closing balance. In effect the auditor will audit this schedule.

As with long term loans owed by the company, the loan should be measured at amortised cost using the effective interest rate. Where the loan is straightforward, e.g. fixed term, no premiums on repayment (by the borrower), the effective rate will be the annual interest rate charged on the loan.

3.1 Valuation - opening balances

* by inspection of prior year working papers, agree opening balances to prior year closing balances.

3.2 New advances (loans)

occurrence, accuracy, cut-off and classification

* inspect directors' minutes for authority to make the loan.
* inspect Memorandum of Incorporation for powers to make loans (including to directors)
* where the loan is made to a ***director*** (or related person etc), confirm by reference to minutes, loan agreement, correspondence that Sec 45 of the Companies Act has been complied with:
  - the liquidity solvency test has been satisfied
  - a special resolution was obtained within the previous two years authorizing the loan (specific or general).
* if the loan is to a related party e.g. subsidiary or holding company, consider whether it is fair and an "arms length" transaction.
* inspect EFT/paid cheque/bank statement/payment records to confirm that the loan was actually made.
* inspect the loan agreement to confirm the following
  - name of borrower
  - client is the lender
  - amount of loan
  - interest rates and repayment terms
  - purpose of loan
  - details of security offered for loan
  - other salient features, e.g. penalties for late payment /any loan covenants.
* confirm by inspection that the amount of the loan reflected in the agreement has been correctly raised in the general ledger.
* inspect the dates on the EFT/paid cheque to confirm that the transaction has been recorded in the correct accounting period.

3.3 Repayments

occurrence, accuracy, cut-off and classification

* inspect cash receipt records/bank statements/deposit slips for evidence of repayments received.
* by inspection of the dates on the receipts, confirm that the repayment has been recorded in the correct accounting period.
* reperform calculations of allocation of repayments into capital and interest portions.
* reperform posting to confirm correct allocation.

3.4 Valuation – closing balance

* reperform casts of the loan summary and general ledger accounts.
* agree the loan summary to general ledger.
* obtain confirmation of the balance owing directly from the party to whom the loan was made and request confirmation of interest rates and any security offered.
* by discussion with the directors, establish whether there is any reason to write down the value of the loan
  - late payment of capital instalment and/or interest
  - notification that the recipient of the loan is in financial trouble e.g. under business rescue, in liquidation.
* recompute the portion of the long-term loan asset which is repayable in the ensuing year and by inspection, confirm that it has been reflected as a current asset.

Note: If there are numerous loans, the client may make an allowance for "bad debts". If this is the case, the provision should be audited in the normal manner (see revenue and receipts Chapter 10).

3.5 Completeness

* review payment records, minutes and correspondence for any evidence of loans advanced which may have been misclassified, particularly in respect of loans to directors.
* send a written request to all directors asking them to confirm details of any loans they or any person/company "related" to them may have received (even if repaid) during the year.
* obtain a written management representation on the completeness of loans advanced.

3.6 Assertions pertaining to presentation and disclosure

* The auditor must inspect the disclosures made and consider
  - whether they are complete in terms of the Companies Act, (e.g. disclosure of deferred interest on loans to directors) and the applicable accounting framework e.g. details of loans to directors and related parties
  - are consistent with evidence gained on the audit
  - amounts, facts, dates etc are accurate and agree with the evidence obtained
  - any classification of the information disclosed is appropriate
  - whether the wording of the disclosures is clear and understandable.

4. INTANGIBLE ASSETS

IAS 38 "Intangible Assets" defines an intangible asset as an "identifiable non-monetary asset without ***physical*** substance ...." Businesses frequently expend resources on acquiring or researching and developing intangible assets such as computer software, patents, copyrights and franchises. The question arises as to how these "investments" in intangibles should be accounted for. IAS 38 is long and detailed and is beyond the scope of this text, but it is important that you have a general idea of how intangibles should be audited. The assertions relating to the "intangibles" balance are the same as for any asset, i.e. ***rights, existence, valuation, completeness.*** Attention will also have to be given to the assertions pertaining to presentation and disclosure. The major risk for the auditor will be ***existence*** and ***valuation***.

4.1 Important accounting aspects

IAS 38 – Intangible assets, states that an intangible asset may only be recognized if, and only if

* it is probable that the expected future economic benefits are attributable to the asset, will flow to the entity, and

* the cost of the asset can be measured reliably.

Simplistically, an intangible asset will either be purchased or internally generated. While the cost of a purchased intangible asset is easier to measure (based on purchase price), the auditor needs to be aware of the guidelines for the recognition of the cost relating to an internally generated intangible asset. With regard to internally generated intangible assets, IAS 38 does not allow any costs incurred in the research phase, to be capitalized. Costs incurred in the development phase may only be capitalized if the following criteria are satisfied

* ***it is technically feasible*** to complete the intangible asset so that it will be available for use or sale.

* the company ***intends*** to complete the intangible asset and use or sell it, and has the ability to use or sell it.

* the intangible asset will ***generate*** probable future economic ***benefits*** (e.g. market research could provide this evidence).

* there are ***adequate*** technical, financial and other ***resources*** available to complete the development of the asset and to sell or use it.

* the company has the ability to reliably ***measure expenditure*** attributable to the intangible asset during its development.

IAS 38 also provides guidance on the amortisation of the intangible asset. An intangible asset should be amortised in a manner that reflects the asset's economic benefits to the entity. If this is not readily determinable, the straight line method may be used. Both the amortization period and the amortization method must be assessed at each reporting date and any changes must be accounted for as a change in accounting estimate. Only intangible assets with finite lives are amortised. Intangible assets with indefinite useful lives are not amortised, however, these assets must be reviewed annually for impairment and whether the assessment that they have indefinite useful lives is appropriate.

Note : While IAS 38 does permit intangible assets to be carried under the revaluation model, they seldom are. This is due mainly to the fact that one of the criteria for use of the model is "an active market", which will often not exist. Further guidance on this can be found in IAS 38.

The following procedures provide guidelines for the audit of intangible assets. As there are many different types of intangible assets, the procedures deal with principles.

4.2 Rights and existence

* where possible inspect documentation which reflects the client's right to the asset, e.g. Letters, Patent, and Certificates of Registration for trademarks, licences.
* inspect documentation for registration in the name of the client and for any endorsements which may impinge on rights.
* if the "intangible" has a "physical" representation, e.g. computer software, or a franchise, it should be inspected by the auditor.

4.3 Completeness

* the risk of understatement is reasonably low so completeness tests may be limited to
  - enquiry of management about research and development projects underway
  - review of minutes, correspondence and disbursement records to identify expenditure on intangibles
  - obtaining written representation from the directors.

4.4 Occurrence, accuracy, cut-off, classification

* The cost of an ***acquired intangible asset*** consists of
  - its purchase price
  - any directly attributable costs of preparing the asset for its intended use e.g. professional fees
* The auditor would
  - inspect the directors' minutes, capital budgets for authority for the purchase
  - inspect the purchase agreements, invoices and payment records pertaining to the purchase to confirm that
    - they are in the name of the company
    - amounts and descriptions agree with what has been recorded
    - the transaction has been recorded in the correct accounting period (dates)
    - all costs included qualify as directly attributable costs e.g. they are ***not*** promotional costs, or general administration costs.
* The cost of an ***internally generated intangible asset*** consists of expenditure incurred during the developmental stage of the asset.
* The auditor would
  - conduct procedures similar to those shown above for acquired intangible assets
  - confirm, by inspection of the supporting documentation for capitalized cost, that the costs were not research costs that should have been excluded (based on the criteria shown under important accounting aspects).

4.5 Valuation - amortisation

Intangible assets have a finite or indefinite useful life. If the company assesses that the intangible asset's useful life is ***finite,*** then the intangible asset must be ***amortised***. If its useful life is considered to be ***indefinite,*** it is ***not amortised***. Therefore the auditor must:

* discuss and evaluate the grounds on which the useful life of the intangible asset was determined.
* where the useful life is classified as finite,
  - confirm that the method of amortisation reflects the pattern in which the intangible asset's economic benefits are consumed by the enterprise, or if this method of amortisation is not possible, the straight-line method has been used.
  - reperform all amortisation calculations.
* where the useful life was classified as indefinite, confirm, by discussion with directors or inspection of supporting schedules or documentation, that the intangible assets have been tested for impairment and that their useful life has been re-assessed.

4.6 Assertions pertaining to presentation and disclosure

The auditor must inspect the disclosures made and consider whether

* they are complete in terms of the applicable accounting framework e.g.
  - whether the useful lives are indefinite or finite
  - amortisation rates and methods
  - gross carrying amounts and accumulated amortisation
  - a reconciliation of the carrying amount at the beginning and end of the period showing additions, increases or decreases from revaluations, impairments, amortisation etc.
  - the reasons supporting the assessment that an intangible asset has an indefinite life.
* they are consistent with evidence gained on the audit.
* amounts, facts, details etc are accurate and agree with the evidence gathered.
* any classification of the information disclosed is appropriate.
* the wording of the disclosures is clear and understandable.

CHAPTER 15

GOING CONCERN AND FACTUAL INSOLVENCY

CONTENTS

		Page
GOING CONCERN		
1.	Introduction	15/2
2.	The auditor's interest in the going concern ability of the client	15/2
3.	The audit plan for going concern	15/3
4.	Obtaining information about going concern	15/5
5.	Mitigating factors and management plans	15/5
6.	Audit conclusions	15/6
7.	The auditor's report	15/6
FACTUAL INSOLVENCY		
1.	Introduction	15/8
2.	The irregularities which may arise when a factually insolvent company continues to trade	15/8
3.	Factual insolvency and sec 45 of the Auditing Profession Act 2005	15/9
4.	Subordination agreements	15/9
5.	Auditing a subordination agreement	15/10

GOING CONCERN

1. INTRODUCTION

1.1 Under normal circumstances, the directors of a company will present the financial statements on the "going concern basis." *This means that assets and liabilities are recorded on the assumption that the company will continue in operational existence for the foreseeable future*. Accordingly, assets and liabilities are recorded on the basis that the entity will be able to realise its assets and discharge its liabilities in the normal course of business.

1.2 The responsibility for the preparation of the financial statements lies with the directors through management. It follows that management should make an assessment of the entity's ability to continue as a going concern when preparing the annual financial statements and in terms of International Accounting Standard IAS 1, management are actually required to make this assessment. Where management is aware of material uncertainties which may cast significant doubt upon the entity's "going concern" ability, the uncertainties should be disclosed. When the financial statements are ***not*** prepared on a going concern basis, this should be disclosed together with the basis on which the financial statements are prepared, and the reason why the company is considered not to be a going concern.

1.3 The extent of management's assessment of "going concern" will vary considerably from entity to entity. Many entities are historically sound and suffer no short term threat to their continued existence. Many others face uncertain futures and extensive assessment of their ability to continue as a going concern may be necessary.

2. THE AUDITOR'S INTEREST IN THE GOING CONCERN ABILITY OF THE CLIENT

2.1 The going concern assumption

As stated above, the going concern assumption is fundamental to the preparation of the financial statements. Whilst going concern itself is not stipulated as an assertion in ISA 315 (revised), the assumption of going concern in the preparation of the financial statements, directly affects many assertions e.g. the value of inventory presented on the going concern basis may differ from the value of the same inventory presented on the liquidation basis. This is because where the company is being liquidated, the inventory may be sold at below cost just to create a cash flow (forced sale). Similarly, a company which is no longer a going concern because the product it sells has become obsolete in the market place, cannot value the plant and equipment which manufactures the product on the going concern basis. In both of the above examples, the valuation assertion is directly affected.

2.2 Audit risk

The risk that the auditor faces is the expression of an unmodified audit opinion where the going concern concept has been, or may have been, applied ***inappropriately***. The possibility of this occurring will vary significantly from client to client. Normally in large listed companies, there is little risk that the company is not a going concern but in other under-resourced companies, it can be a real risk. Regardless of the auditor's initial impressions of the client's going concern ability, sufficient appropriate evidence will still have to be gathered to support the adoption, by the client, of the going concern assumption in the preparation of the financial statements.

Looking at it another way, if the financial statements are presented on the going concern basis when the company is not a going concern, there will be ***material misstatement*** in the financial statements which the auditors cannot ignore.

2.3 Auditor's objectives

The auditor's objectives with regard to going concern are

* to obtain sufficient appropriate evidence about the appropriateness of management's use of the going concern assumption in the preparation of the financial statements
* to conclude, based on the evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the entity's ability to

continue as a going concern

* to determine the implications for the audit report.

2.4 When does the auditor consider the appropriateness of "going concern"?

The audit is an ongoing evidence gathering exercise and pieces of evidence relating to going concern will be obtained at all stages of the audit:

* during ***planning (risk assessment procedures):*** in terms of ISA 570 – Going Concern, the auditor must carry out risk assessment procedures specifically relating to the going concern ability of the entity. This will be part of identifying and assessing the risk of material misstatement (ISA 315 (Revised)). In particular, the auditor should consider any material uncertainties with regard to events or conditions and related business risks which may cast significant doubt upon the entity's ability to continue as a going concern.

* during the ***performance of further audit procedures:*** if the risk assessment procedures have raised concerns about "going concern", the auditor will carry out specific further audit procedures to respond to the risk. In addition, when carrying out further audit procedures not specific to going concern, the auditor should be ***alert*** to events or conditions which provide evidence (negative or positive) relating to going concern. For example, when auditing accounts payable, the auditor might notice an increasing number of complaints from creditors about slow or erratic payment from the client. This does not mean there is a going concern problem, it simply provides an additional piece of evidence which may cause the auditor to re-assess the risk relating to going concern.

* ***other audit procedures to comply with ISA 570*** : the risk assessment procedures may indicate that there is minimal risk relating to going concern. However, the auditor is still required to carry out procedures to confirm this initial assessment so as to comply with the ISAs. These ***other*** procedures may be quick and easy but they must be done.

* as part of the ***review of subsequent events:*** the auditor will identify and evaluate the effect, if any, which subsequent events may have had on going concern. For example if the client's major market collapses during the post reporting period, it will certainly influence the auditor's opinion on whether the going concern basis is appropriate. The post reporting period may also provide further evidence of events or conditions affecting going concern which were identified prior to year-end.

* at the ***evaluating and concluding stage:*** at this stage the auditor considers all the individual pieces of evidence gathered relating to going concern, ***collectively***.

As indicated in the introduction, management should have carried out an assessment of the company's going concern ability. This will be useful to the auditor, and ISA 570 requires that the auditor evaluate management's assessment.

3. THE AUDIT PLAN FOR GOING CONCERN

The directors through management are charged with the responsibility of assessing their company's ability to continue as a going concern. In making their assessment, management must take into account all available information about the future, which is "at least, but not limited to, twelve months from the reporting date". The assessment may be made for a longer period but the degree of uncertainty associated with future events, increases the further management looks into the future.

The nature, timing and extent of tests conducted by the auditor will depend primarily on the level of risk which the auditor perceives exist, in respect of the adoption by the directors of the going concern basis of preparation. ***The risk assessment procedures*** will be conventional: i.e.

* inquiries of management and others within the entity
* analytical procedures e.g. analysis of related ratios
* inspection of documentation e.g. management reports, cash flow forecasts, budgets, the state of the company's order book.

With regard to ***further and other procedures***:
The ***nature*** of testing will be a substantive evaluation of management's assessment of the entity's ability to continue as a going concern, predominantly the application of analytical procedures, confirmation of evidence provided by management, and enquiry of personnel. The "audit" of going concern is not necessarily simple, as it requires the auditor to evaluate not only historical data, but also, where going concern is in doubt, a client's survival strategy and forecasts must be evaluated. Strategies and forecasts are by their nature, subjective. Where going concern has been assessed by management for the following twelve months (normally the case) the auditor should still enquire as to whether management is aware of anything beyond the twelve months which may cast significant doubt on the entity's ability to continue as a going concern.

The ***extent*** of testing will vary directly with the "certainty" of the company's ability to continue as a going concern. Little specific going concern audit work will be required for a sound, liquid and solvent company, whereas a great deal of going concern audit work may be required where the company is facing an uncertain future, and where there are material uncertainties.

The ***timing*** of testing will of necessity centre around the financial year end and the post reporting date period. This is due to the fact that the auditor in interested in the most current up to date information about the company's going concern ability.

The explanatory notes to ISA 570 - Going Concern, provides an analysis framework and examples of events or conditions which may cast doubt about the entity's ability to continue as a going concern, specifically ***financial***, ***operating*** and ***other*** events or conditions. Particularly in a situation where these events or conditions suggest that going concern is at risk, ***mitigating factors*** (factors which reduce the risk) should also be considered.

3.1 Financial

* the company is in a net liability or net current liability position
* fixed term borrowings are approaching maturity without realistic prospects of renewal or repayment
* excessive reliance on short- term borrowings to finance long-term assets
* indications of withdrawal of financial support by suppliers and other creditors
* adverse key financial ratios
* negative operating cash flows
* substantial operating losses or significant deterioration in the value of assets used to generate cash flows
* arrears or discontinuance of dividends
* inability to pay creditors on due dates
* difficulty in complying with the terms of loan agreements
* change from credit to cash-on-delivery transactions with suppliers
* inability to obtain financing for essential new product development or other essential investments.

3.2 Operating

* management intentions to liquidate the entity or to cease operations
* loss of key management without replacement
* loss of a major market, franchise, licence, or principal supplier
* labour difficulties e.g. strikes, go slows, lack of skills
* shortage of important supplies e.g. raw materials
* technological obsolescence of products
* threats from cheap imported goods
* emergence of a highly successful competitor.

3.3 Other

* pending legal proceedings against the entity which may, if successful, result in judgements which cannot be met, e.g. extensive damages awarded against the client
* changes in legislation or government policies e.g. withdrawal of tax concessions, banning of client's product
* negative perceptions about the company's product in the market place

* failure to satisfy Black Economic Empowerment requirements leading to the loss of contracts.

3.4 Mitigating factors

* plans made by management to counterbalance the effects of negative events or conditions, e.g. detailed cash flows reflecting a return to profitable trading or the planned sale of redundant assets to create a cash flow
* potential support from a holding company or fellow subsidiary
* a record of managing going concern crises successfully.

4. OBTAINING INFORMATION ABOUT GOING CONCERN

Information about going concern will come from the auditor's consideration of management's assessment of the entity's ability to continue as a going concern, by analytical review, enquiry and confirmation, as well as the auditor's own evidence gathered throughout the audit. More specifically the auditor should:

4.1 Analyse and discuss cash flow, profit and other relevant forecasts with management.

4.2 Analyse and discuss the entity's most recent available interim financial information.

4.3 Review the terms of debentures and loan agreements to determine whether they have been and can be met (have not been breached).

4.4 Read minutes of meetings of shareholders and those charged with governance, (directors and the audit committee) for reference to financial difficulties.

4.5 Enquire of the entity's lawyers regarding litigation and claims, and the reasonableness of management's assessment of any financial implications for the company.

4.6 Confirm the existence, legality and enforceability of arrangements to provide or maintain financial support with related and third parties and assess the financial ability of such parties to provide additional funds.

4.7 Consider the entity's position concerning unfilled customer contracts/orders, e.g. penalties for failure to perform.

4.8 Review events after year-end for transactions or events which either mitigate or aggravate conditions affecting the entity's ability to continue as a going concern.

5. MITIGATING FACTORS AND MANAGEMENT PLANS

5.1 When faced with a material uncertainty regarding their company's ability to continue as a going concern, the directors will attempt to put plans in place to resolve the problem. Common "management plans" are:

* the disposal of assets to generate a cash flow
* raising of additional capital or restructuring debt
* cost cutting
* increasing sales

5.2 The auditor obviously has a duty to consider any plan which management offers, as the plan is, in effect, a mitigating factor. In this regard the auditor:

* should gather sufficient appropriate evidence that the plans are ***specific*** and ***feasible***. For example, a plan to "increase sales volume by 25%" would have to be supported by specific detail as to how this is going to be achieved. The auditor will need to "audit" the detail and consider whether, in the light of the evidence gathered, the plan can be achieved (feasible). For example, a manufacturing company which is going to "increase sales volume by 25%" will need sufficient production capacity to meet the increased sales. If it does not have the capacity, the plan is not feasible.
* should pay careful attention to the underlying assumptions which management use in their

plans. By their nature, assumptions are subjective so the most that the auditor can do, is to evaluate whether the assumptions are appropriate, reasonable, suitably supported and not vague generalities. Increasing sales by 25% sounds good but how does the entity do it!

* must realise that most plans will have a negative side to them which could increase the going concern problem! For example, most plans which create a cash ***inflow***, create a cash ***outflow*** as well; if a new loan is negotiated (inflow), interest and ultimately the capital sum must be paid to the loan provider (outflow). Another example might be where retrenchments are planned as a cost cutting exercise; not only does this create an outflow (retrenchment packages), but the company's ability to service its customers may also be negatively affected resulting in customers taking their business elsewhere.
* should ensure that the directors provide written representation regarding their intentions to commit to the plan, and that the directors have approved the plan and are committed to it.

6. AUDIT CONCLUSIONS

6.1 After sufficient appropriate evidence has been obtained relating to the going concern assumption, the auditor must decide whether a ***material uncertainty*** exists that may cast significant doubt upon the entity's ability to continue as a going concern. A material uncertainty exists when the magnitude of its potential impact is such that clear ***disclosure*** of the nature and implications of the uncertainly is necessary for the presentation of the financial statements not to be misleading.

6.2 If a ***material uncertainty*** exists it must be properly disclosed in the financial statements otherwise the financial statements do not fairly present the state of the affairs of the company.

6.3 Proper ***disclosure*** requires that the financial statements:

* adequately describe the conditions that give rise to the significant doubt (material uncertainty) about the entity's ability to continue in operation for the foreseeable future, and management's plans to deal with these events or conditions.
* state clearly that there is a material uncertainty related to events or conditions which may cast significant doubt about the entity's ability to continue as a going concern, and therefore, that it may be unable to realise its assets and discharge its liabilities in the normal course of business.

7. THE AUDITOR'S REPORT (assuming there are no other reporting issues)

The auditor has a number of possibilities to consider in deciding on the appropriate audit report:

7.1 Unmodified opinion

If no doubt exists relating to the appropriateness of presentation of the AFS on the going concern basis, an ***unmodified audit report*** will be given.

7.2 Unmodified opinion - emphasis of matter added

This report is given when:

* the going concern basis of presentation ***is*** appropriate but
* a material uncertainty that may cast significant doubt about the company's ability to continue as a going concern exists and
* the material uncertainty is ***properly disclosed*** (see 6.3 above)

The emphasis of matter must highlight the existence of the material uncertainty and draw attention to the note in the financial statements.

7.3 Qualified opinion or adverse opinion based on disclosure problems

This report is given when:

* the going concern basis of presentation ***is*** appropriate but
* a material uncertainty that may cast significant doubt about the company's ability to continue as a going concern exists and
* the material uncertainty has ***not*** been disclosed or has been ***inadequately*** disclosed.

This situation amounts to a disagreement with the directors on disclosure and hence can only result in an "except for" qualified opinion or an adverse opinion.

* the "***except for***" qualified opinion will be given where in the auditor's judgement, the

disagreement on disclosure is ***not*** so material and pervasive as to require an adverse opinion

* the ***adverse opinion*** will be given when the effect of the failure to disclose or adequately disclose the going concern problem, is so material and pervasive that the auditor concludes that an "except for" qualification of the report is not adequate to reflect the misleading and incomplete nature of the financial statements.

How the auditor distinguishes between material (except for) and material and pervasive (adverse) with regard to going concern is a matter of professional judgment. It has been suggested that if the differences between the amounts in the financial statements presented on the going concern basis, are not material when compared to the same amounts presented on the liquidation basis, an except for opinion could be given. This argument overlooks the fact that the basis of presentation is incorrect and focuses only on the values actually assigned to the assets and liabilities, and is therefore ***not*** theoretically sound.

Another suggestion for making the distinction is the extent of the disclosure. If say, 60% of the relevant facts about the going concern problem have been disclosed, an "except for" opinion could be given, whereas if only say, 20% of the facts have been disclosed, an adverse opinion is given! The basis of this suggestion is that 60% disclosure, whilst inadequate, alerts the user to the problem but 20% disclosure results in financial statements which are incomplete and misleading, and therefore should not be relied upon because the seriousness of the going concern problem has not been adequately conveyed.

The question the auditor must answer is whether or not the omission or lack of (inadequate) disclosure renders the financial statements incomplete or misleading to the extent that fair presentation has not been achieved. If it does, an adverse opinion must be given.

7.4 Adverse opinion – inappropriate basis

This report is given when:

* the financial statements are presented on the going concern basis ***but***
* in the opinion of the auditor, this basis is ***not*** appropriate ***regardless of whether or not*** proper disclosure has been made of the material uncertainties.

When the auditor concludes that the going concern assumption used in preparation of the financial statements is ***not*** appropriate, i.e. the company will not be able to continue as a going concern, an ***adverse opinion*** must be expressed. If, on the basis of the procedures carried out and all the information obtained, including the effect of management's plans, the auditor's judgment is that the entity will not be able to continue as a going concern, the auditor must express an adverse opinion, ***regardless of whether or not disclosure of the going concern problem has been made***.

7.5 Disclaimer of opinion

This report is given when:

* the financial statements are presented on the going concern basis and
* proper disclosure of material uncertainties has been made ***but***
* the auditor is unable to form an opinion as to whether this is the appropriate basis due to the presence of multiple significant uncertainties. (This is considered to be a very rare occurrence by ISA 570.)

ISA 570 – Going Concern, recognises that there may be "extreme" cases where there are multiple material uncertainties, which have all been adequately disclosed ***but*** the auditor is ***unable to decide*** whether "going concern" is the appropriate basis of presentation. In this instance ISA 570 states that the auditor may give a disclaimer of opinion instead of an emphasis of matter. (Remember that the use of an "emphasis of matter" assumes that going concern ***is*** the appropriate basis of presentation.) The effect of multiple material uncertainties is almost like a limitation of scope, the auditor cannot gather enough evidence (for whatever reason) to form an opinion.

ISA 570 suggests that there may be situations where the auditor is limited in his scope when auditing going concern, e.g. management may not co-operate in supplying relevant information or may refuse to provide its own assessment of the company's going concern ability. This situation would have to result in a qualification based on a limitation of scope (insufficient evidence).

FACTUAL INSOLVENCY

1. INTRODUCTION

For the purposes of this topic there are two categories of insolvency to consider:

1.1 ***Commercial insolvency*** arises when an undertaking is unable to pay its debts as they fall due as a result of illiquidity, even though its assets may exceed its liabilities.

1.2 ***Factual insolvency*** arises when the liabilities of an undertaking exceed its assets, fairly valued.

Commercial insolvency would clearly indicate going concern problems and would be taken into consideration by the auditor in assessing the appropriateness of presenting the AFS on the going concern basis.

Factual insolvency also clearly indicates going concern problems but, in addition, has far more serious implications for the auditor. Where a company continues to trade when its liabilities exceed its assets, fairly valued, a situation is created where certain irregularities may be taking place. If such irregularities are taking place, a duty on the part of the auditor to report a "reportable irregularity" as contemplated by Sec 45 of the Auditing Profession Act 2005, may arise. The mere fact that the company continues to trade whilst factually insolvent is not in itself, an irregularity, but a situation is created which may give rise to certain irregularities.

2. THE IRREGULARITIES WHICH MAY ARISE WHEN A FACTUALLY INSOLVENT COMPANY CONTINUES TO TRADE

2.1 ***Common law fraud***

The crime of fraud includes *unlawfully making, with intent to defraud, a misrepresentation that causes actual prejudice to another.* In the context of this topic, the directors of a company which is factually insolvent, may be guilty of fraud, if for example, they enter into a contract with a supplier of goods knowing that the goods supplied will not be paid for.

2.2 ***Reckless trading –Companies Act 2008 Section 22***

In terms of Sec 22 “a company must not carry on its business recklessly, with gross negligence, with intent to defraud any person or for any fraudulent purpose”. When a company is factually insolvent is it “reckless” for the directors to continue trading? Obviously there is a fair amount of subjectivity in determining whether the directors have been ***reckless*** but the key will be to determine whether the directors have acted as ***reasonable people***. The question to be answered is whether a reasonable person would have acted in the same manner under a situation of factual insolvency. An example may better illustrate this. Assuming the company is factually insolvent, would it be ***reasonable*** for a company to enter into a lease agreement for a very expensive fleet of company vehicles for its directors to drive about in? Alternatively, would it be ***reasonable*** for three or four directors to embark on an extensive overseas trip to visit trade fairs when one director could make the trip? Would it be reasonable for the directors to vote themselves large bonuses or substantial salary increases?

Furthermore if the directors of a factually insolvent company, continue to incur debts when there is, to the knowledge of the directors, no reasonable prospect of the creditors ever receiving payment for those debts, a breach of Sec 22 will probably have taken place.

2.3 ***Summary***

Where a company is factually insolvent, there is a greater risk that common law fraud, recklessness or gross negligence could occur. If any of the above have occurred (or are occurring) an unlawful act will have taken place. If the other requirements for a reportable irregularity are present (Sec 1 – definitions. Auditing Profession Act 2005) a duty in terms of Section 45 will have arisen. The auditor must report accordingly to the IRBA.

3. FACTUAL INSOLVENCY AND SEC 45 OF THE AUDITING PROFESSION ACT (reportable irregularities)

As indicated above, trading whilst factually insolvent may give rise to a reportable irregularity. In terms of AP Act Sec 1 – Definitions, to be a reportable irregularity the matter must be

3.1 ***An unlawful act or omission*** – the mere fact that a company is trading whilst factually insolvent is not itself unlawful. (See note below.) However, if fraud or any Companies Act Sec 22 contraventions are underway, an unlawful act will have occurred.

Note: In the original version of the Companies Act 2008, Sec 22 stated that "a company must not trade under insolvent circumstances" suggesting that to do so would constitute an unlawful act. However, an amendment to the Act in 2011 removed this "prohibition" leaving only the prohibition of reckless trading, gross negligence and intention to defraud.

3.2 ***Committed by management*** – if fraudulent/reckless acts are being committed in this context, it will be as a result of decisions taken by those responsible for the management of the company.

3.3 The section goes on to say that the unlawful act must

* have caused or be likely to cause financial loss ***or***
* be fraudulent or amount to theft ***or***
* represent a material breach of fiduciary duty by the person committing the unlawful act.

Note the use of the word "or". Although there will usually be financial loss if fraud, recklessness or gross negligence has taken place, financial loss is not a requirement that has to be satisfied before the matter becomes a reportable irregularity. Regardless of financial loss, if the act is fraudulent the requirements for a reportable irregularity are satisfied. In addition it should be noted that to commit fraud, or to intend to commit fraud, is likely to represent a material breach of fiduciary duty on the part of the directors.

Thus if a company continues to trade whilst its liabilities exceed its assets fairly valued, and in doing so the directors act fraudulently or recklessly in carrying on the business of the company (regardless of financial loss), a duty to report in terms of Sec 45 of the AP Act arises.

Once the auditor has made the first report to the Regulatory Board, the matter must "as soon as possible" be discussed with the directors. Essentially the directors will have to provide the auditor with evidence that they have not carried on the business of the company fraudulently or recklessly.

In deciding whether the directors have acted unlawfully, the auditor will need to evaluate the evidence presented by the directors to refute the allegations and will probably need to obtain legal opinion. Remember from a going concern perspective, the auditor will certainly take the insolvency into account, but from a reportable irregularity perspective, the auditor is more concerned about whether the directors have acted fraudulently, recklessly (with gross negligence) or have breached their fiduciary duty. Should the auditor fail to obtain the necessary evidence (to refute this), he must report to the IRBA that the reportable irregularity is continuing. The second report to the IRBA must be made within 30 days of the first report.

4. SUBORDINATION AGREEMENTS (ALSO CALLED BACKRANKING AGREEMENTS)

4.1 ***A common step which is taken by directors of factually insolvent companies in an attempt to get their companies back to health, is to obtain a backranking agreement. This is defined as:***

An agreement by a substantial creditor(s) whereby that creditor binds itself either ***indefinitely*** or for a ***limited period***, ***conditionally*** or ***unconditionally*** not to ***claim*** or ***accept*** payment of the amounts owing to it until the happening of a particular event.
The idea is that the factually insolvent company is given a "breathing space" during which time it can get itself back to a satisfactory level of financial stability. Whilst a backranking/subordination agreement does not create an inflow of funds, it delays outflows which in effect may assist the company's liquidity.

4.2 Why would a creditor subordinate (backrank) the amount it is owed by the factually insolvent company?

Remember we are dealing with a company whose liabilities exceed its assets and whose creditors will therefore not be paid in full if the company is liquidated. A creditor may believe that, in the long run, it will be a better business decision to keep the insolvent company functioning in the hope of ultimately being paid in full, than to allow liquidation to take place. There may, of course, be other reasons why the creditor company may wish to keep the insolvent company alive, for example, the insolvent company may be part of a group or may possess some unique characteristic, such as a non-transferable license to manufacture a particular product.

4.3 Audit considerations with respect to subordination agreements.

* A subordination agreement is an important piece of evidence for the auditor. A valid subordination agreement may be significant in determining whether the ***going concern basis of presentation is appropriate***. Indeed, the agreement may be the very reason that the company is able to continue in operational existence. For example, a holding company may subordinate its loan to its subsidiary until the subsidiary returns to profitable trading. Other creditors will be more inclined to continue supplying the subsidiary and trading can continue. However, the presence of a subordination agreement does ***not*** automatically mean that the factually insolvent company will be a going concern, it is simply a mitigating factor - ***financial, operating and other factors must still be considered.***

* In relation to the situation where the auditor considers whether a reportable irregularity is taking place, the subordination agreement has no specific significance other than if it is presented as part of the evidence produced by the directors to prove they have not acted fraudulently or recklessly. The directors may contend that they are not being fraudulent, negligent or reckless in their actions, but are acting responsibly and are fulfilling their fiduciary duty by acting in the best interests of the company by obtaining a subordination agreement.

5. AUDITING A SUBORDINATION AGREEMENT

***The following considerations should be taken into account when auditing a subordination agreement*:**

5.1 The contract

* The auditor must be satisfied that the contract:
  - is in writing in the format recommended by SAICA
  - is signed by the creditor (with due authority)
  - is between the client and the creditor
  - is accepted by the client (signed by the directors)
  - complies with all legal formalities.

5.2 Size

* The auditor must be satisfied that the claim which is backranked (subordinated) is of sufficient size to create a situation where exception cannot be taken to a continuation of trading. ***Remember***: The intention of backranking is to give the company a realistic chance to recover - not simply to get the "accounting" right. The backranking creditor (the amount backranked) must be large enough for this concession to have some effect.

5.3 Financial substance of the backranking creditor

* The auditor must consider whether the backranking creditor is (financially) of ***sufficient substance***.
  - should the backranking creditor go insolvent, every disposition of property ***not made for value*** may be set aside by the liquidator of that company if, immediately after the disposition, the liabilities of the insolvent (creditor company) exceed its assets.
  - the auditor must therefore assess the possibility of insolvency of the creditor giving the backranking agreement, and whether ***value*** has, in fact, been received by the creditor. If there is a possibility of the subordination agreement being set aside, the auditor will be concerned about its suitability as acceptable evidence.

Note: We are dealing here with the insolvency of the party which is ***subordinating*** (backranking) its claim. In effect by subordinating its claim this party is "disposing" of its right to one of its assets and if no value is received in return, the disposition may be set aside under the circumstances outlined above. (This is a principle in insolvency law.)

5.4 Creditors right to backrank

* The auditor must also determine by written enquiry, whether the backranking creditor is entitled to backrank the debt e.g. the debt may have been offered as some form of security to another party.

5.5 Reversal of the backranking agreement

* The auditor must be aware of the possibility of the reversal of the subordination agreement after it has been presented as evidence in support of the adoption of the going concern assumption and should therefore give consideration to the integrity of the parties to the agreement and be quite clear about their intentions. Is it a genuine attempt to save the company?

5.6 3rd Party acceptance

* The auditor should determine by inspection of correspondence and discussion with the directors as to whether any creditors (3rd parties) of the client company have accepted the benefit of the subordination agreement. For example, a supplier may have agreed to supply goods to the insolvent company because of the existence of the subordination agreement. This gives more credibility to the subordination agreement as it cannot simply be legally reversed without the consent of the third party (creditor).

5.7 Documentation

* The original of the subordination agreement should be retained by the provider of the agreement and a true copy by the client company. The auditor should also retain a copy in the audit documentation.

5.8 Disclosure

* The entire matter should be fully disclosed by way of note and suitably described in the statement of financial position. Usually this will mean that the backranked creditor will be shown as a separate long-term liability (non-current liability) in the company whose creditor is backranked, and as a separate "long-term" debtor in the company which is backranking its claim. As the subordination agreement relates to going concern, failure to make proper disclosure, will result in a qualified or adverse opinion. Proper disclosure will result in an “emphasis of matter” modification.

CHAPTER 16

RELIANCE ON OTHER PARTIES

CONTENTS

		Page
INTRODUCTION		16/2
ISA 600 – SPECIAL CONSIDERATIONS – AUDITS OF GROUP FINANCIAL STATEMENTS (INCLUDING THE WORK OF COMPONENT AUDITORS)		16/2
1.	Introduction	16/2
2.	Responsibilities of the group engagement partner with regard to the component auditor	16/3
3.	Reporting considerations	16/5
ISA 610 (Revised 2013) – USING THE WORK OF INTERNAL AUDITORS		16/5
1.	Introduction	16/5
2.	Definition of the Internal Audit Function	16/5
3.	External Auditor's objectives	16/6
4.	External Auditor's responsibility	16/5
5.	Evaluating the internal audit function	16/6
6.	Determining the nature and extent of the internal audit function that can be used	16/7
7.	Using the work of the internal audit function	16/8
8.	Determining whether internal auditors can be used to provide direct assistance	16/8
9.	Using internal auditors to provide direct assistance	16/9
10.	Documentation	16/10
ISA 620 – USING THE WORK OF AN AUDITOR'S EXPERT		16/10
1.	Introduction	16/10
2.	Definition of an auditor's expert	16/10
3.	Determining the need for an auditor's expert	16/10
4.	Determining the need to use an auditor's expert when management has used a management's expert	16/11
5.	Nature, timing and extent of audit procedures	16/11
6.	Reference to the auditor's expert in the auditor's report	16/13

INTRODUCTION

There are many instances where an auditor, appointed by a client to provide audit assurance, will find it effective and efficient to engage other parties to gather evidence on which he can rely when forming the audit opinion. Common examples of parties on which an auditor may rely are

* ***Other firms of auditors***
  This is most common where a group engagement partner (the partner responsible for the audit of a group of companies), relies on the work of another firm of auditors who have audited a component of the group, e.g. a subsidiary within the group. Another common example is where the auditor of the company engages another auditor (or firm) to observe an inventory count or conduct a physical asset verification at a branch or division of the company which is in a distant location (but close to the other audit firm), because it is more cost effective and efficient than sending his own audit team to that location.

* ***Internal auditors***
  Many companies, particularly large companies, have highly competent internal audit departments which operate independently of management and which carry out functions which can be of real assistance to the external auditor. For example, modern internal audit is risk based which requires that internal audit has a detailed knowledge of the risks faced by the company. External audit is also risk based, so, although internal and external audit do not have exactly the same objectives, there is plenty of common ground between the two. It makes sense that if the external audit strategy can justifiably include some reliance on internal audit, a more effective and efficient audit may result.

* ***An auditor's expert***
  In some situations an auditor may need the expertise of another individual to assist him in gathering sufficient appropriate evidence pertaining to a particular assertion relating to the financial statements. For example, the valuation of inventory in a chemical company, or the legal interpretation of a contract, may be beyond the expertise of the auditor and may require that the auditor rely on the expertise of a chemical engineer or a lawyer.

However, it is important to remember that the auditor has sole responsibility for the audit opinion, and that responsibility is not reduced because another party (other auditor, internal auditor or auditor's expert) was involved in obtaining evidence. In other words the auditor does not ***escape responsibility*** for assessing the suitability of the evidence provided by the other party, he must therefore assess both the ***party*** and the ***evidence*** provided. In effect the other party can be regarded as an extention of the audit team and must possess the same professional attributes as the auditor. The evidence gathered by the other party must be sufficient and appropriate.

This means that the work carried out by the other party e.g. an auditor's expert, must be performed or supervised by a person having adequate ***skills and competence*** and who meets the professional requirements of ***independence, objectivity, confidentiality*** and ***professional behaviour***. This also means that the evidence gathered must be ***sufficient, relevant and reliable.***

The three International Standards on Auditing relevant to reliance on other parties are dealt with below.

ISA 600 – SPECIAL CONSIDERATIONS – AUDITS OF GROUP FINANCIAL STATEMENTS (INCLUDING THE WORK OF COMPONENT AUDITORS)

1. Introduction

ISA 600 does not deal exclusively with reliance by an auditor on other auditors. As the title indicates, the statement deals with special considerations with regard to the audit of group financial statements. One of those special considerations is the reliance by the group engagement partner (i.e. the auditor responsible for giving the opinion on the group financial statements), on other auditors who may have audited a "component" of the group financial statements. The simplest way of understanding this is to think about a holding company with a number of subsidiaries where some of the subsidiaries are audited by audit firms other than the firm which audits the holding company. As you will know, the subsidiary financial statements and the holding company financial statements are consolidated and the holding company auditor is required to pass an audit opinion on the fair presentation of the consolidated financial statements. Thus we have the group engagement partner having to rely on the work of the component auditor, i.e. the subsidiary company auditor in this case. Note that a component will not necessarily be a subsidiary

company, it could be any entity or business activity for which financial information is incorporated into the group financial statements, e.g. a joint venture, or separate division.

Despite concentrating on component auditors in a group situation, ISA 600 makes the point that the statement "may be useful" when the auditor involves "other auditors" in the audit of financial statements that are not group financial statements, for example where an auditor involves another auditor to observe an inventory count at a location which is convenient to the "other auditor" but not to the auditor himself.

The summary that follows will consider the principles of reliance on other auditors in the context of a group engagement partner and a component auditor, but you should recognise that these principles apply equally to other situations where an auditor who has been assigned a responsibility, relies on the work of another auditor to assist in meeting that responsibility.

The principle here is simple. If an auditor relies upon other auditors, he is entitled to assess the other auditors and their performance to the extent he considers necessary, much in the same manner that the auditor would assess his own audit team. The other auditors are simply an extension of the audit team. The auditor is not entitled to ***assume*** that the other auditor has the necessary ***technical ability and competence***, or fulfils the necessary ***professional requirements***.

2. Responsibilities of the group engagement partner with regard to the component auditor

2.1 Overall responsibility

The group engagement partner is responsible for the direction, supervision and performance of the group audit engagement in compliance with the auditing standards and any legal/regulatory requirements. It is the responsibility of the group engagement partner to obtain sufficient appropriate evidence on which to base his opinion.

2.2 Overall audit strategy and audit plan

Determining the overall audit strategy and developing the audit plan for the group audit is the responsibility of the group audit engagement team and the group audit engagement partner. Frequently, in group audit situations, the audit strategy will include reliance on component auditors and the audit plan will need to accommodate this.

Where the use of a component auditor is included in the audit strategy, the engagement partner (team) must obtain an understanding of:

* whether the component auditor understands and will comply with the ethical requirements of the group audit, e.g. independence, confidentiality
* the component auditor's professional competence, e.g. has the necessary skills, knowledge and experience
* whether the group engagement team will be able to be involved in the work of the component auditor
* whether the component auditor operates in an environment in which auditors are actively regulated (note: the component auditor may be from another country).

This understanding may be acquired by

* discussion with the component auditor
* requesting written submissions from the component auditor relating to the matters listed above
* requesting the component auditor to complete questionnaires designed to obtain this information
* discussing the component auditor with colleagues or a reputable and knowledgeable 3rd party
* obtaining information from the component auditor's professional body.

2.3 Risk assessment procedures and response

Where the component auditor performs an audit on a significant component (a component that is of individual financial significance to the group, or is likely to include significant risks of material misstatement), the group audit partner (team) must be involved in the component auditor's risk assessment procedures. This will include as a minimum

* discussing with the component auditor the susceptibility of the component's financial information to material misstatement due to fraud or error and
* reviewing the component auditor's documentation of identified risks of material misstatement.

Where significant risks of material misstatement of the group financial statements have been identified in a component on which the component auditor performs the work, the group engagement partner (team) shall evaluate the appropriateness of the further audit procedures to be performed to respond to the risks.

2.4 Communication with the component auditor

The group engagement partner (team) must convey its requirements to the component auditor on a timely basis. The communication must set out

* the work to be performed, the use to be made of that work and the form and content of the component auditor's communication with the engagement team, and
* a request that the component auditor confirm that the component auditor will co-operate with the group engagement team
* the ethical requirements relevant to the group audit, particularly independence
* component materiality and the threshold above which misstatements cannot be regarded as clearly trivial to the group financial statements
* identified significant risks of material misstatement due to fraud or error which are relevant to the component auditor
* a list of related parties, and a request to the component auditor to communicate knowledge of any related parties not on the list.

2.5 Communication by the component auditor

With regard to communication by the component auditor with the group engagement team, the engagement partner (team) should request the component auditor to communicate the following (in writing)

* whether the component auditor has complied with the ethical requirements including independence and professional competence
* whether the component auditor has complied with the group engagement team's requirements in respect of the work to be performed
* identification of the financial information on which the component auditor is reporting
* information on instances of non-compliance with laws and regulations that could give rise to material misstatement of the group financial statements
* a list of uncorrected misstatements (excluding those below the "trivial" threshold)
* any indication of (component) management bias at the component entity
* a description of significant internal control deficiencies at component level
* significant matters identified e.g. suspected fraud at the component
* any other matters to which the component auditor wishes to draw the attention of the group engagement partner
* the component auditor's overall findings, conclusions or opinion.

2.6 Evaluating the sufficiency and appropriateness of audit evidence obtained

The group engagement partner (team) must evaluate the component auditor's communication and the adequacy of his work

* conventional "evaluation of work papers" techniques will be used e.g. review, discussion, checking for consistency, analytical procedures
* any significant matters arising from the evaluation of the component auditor's communication will be discussed with the component auditor
* if the group engagement team concludes that the work of the component auditor is insufficient, the team must determine what further work must be done and who will do it.

2.7 Communication with those charged with governance

The group engagement partner (team) must communicate with those charged with governance of the group, any important matters relating to the component auditor's work, e.g.

* an overview of the type of work to be performed on the financial information of the component
* an overview of the nature of the group engagement team's planned involvement in the work to be preformed by the component auditors on the financial information of significant components
* instances where the group engagement team's evaluation of the component auditor's work

gave rise to concern relating to the quality of the work (and responses thereto)
* instances where access to component information may have been restricted
* fraud or suspected fraud at the component.

3. Reporting Considerations

Where an auditor has relied on the work of another auditor when forming his opinion, ***no*** mention of this fact will be made in the audit report. The responsibility for giving the opinion rests with the auditor and making reference to the fact that the auditor has relied on other auditors may give the impression to users of the report that the auditor is attempting to shift responsibility to the other auditor.

ISA 610 (Revised) – USING THE WORK OF INTERNAL AUDITORS with reference to the King III Report

1. Introduction

The practice of internal auditing has been around for many years but its scope, nature, form and importance have evolved considerably. Before this evolution, internal audit departments were frequently understaffed, ill-equipped and more of a "general assistance" department to be called upon for help when the accounting department was short-staffed or very busy. However, modern day internal audit is a different story. In most large companies, internal audit is respected and effective. Internal auditors are well qualified (many are chartered accountants with extensive external audit experience), well supported resource-wise, and regulated by their own professional body, the Institute of Internal Auditors.

It is perhaps true to say that the evolution of internal audit was driven by the focus on improving corporate governance. As part of a large company's overall assurance model, internal audit, along with external audit (and other external regulatory inputs), is ideally placed to make a significant contribution to sound corporate governance. This idea has been recognized in the King III Report on corporate governance and calls for company boards to ensure that there is an effective internal audit function.

ISA 610 (Revised 2013) – Using the work of internal auditors, deals with the external auditor's responsibilities when ***using the work*** of internal auditors, including using the work of internal auditors in obtaining audit evidence, and using internal auditors to provide ***direct assistance*** under the direction, supervision and review of the external auditor. Note that the ISA does not ***require*** the external auditor to make use of internal audit in any way. This decision will be made by the external auditor when establishing the overall audit strategy and audit plan, and will be based on whether it would be efficient and effective to do so. Of course, the independence and competence of the internal audit department would also be very important in making the decision, and ISA 610 requires that the internal audit function be carefully evaluated.

2. Definition of the Internal Audit Function – ISA 610

The objectives and scope of internal audit functions typically include assurance and consulting activities designed to evaluate and improve the entity's governance processes, risk management and internal control.

* ***Governance.*** The internal audit function may assess the governance process in terms of whether objectives relating to ethics, performance, management and accountability, communication with stakeholders etc, are being met.
* ***Risk management.*** The internal audit function may assist by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management (response) and internal control. Internal audit assists in the detection of fraud.
* ***Internal control.*** The internal audit function may be assigned to review controls, evaluate their operation and recommend improvements. It may also examine financial and operating information, including detailed testing of transactions, balances and procedures.

In addition, internal audit may be assigned to review the economy, efficiency and effectiveness of operating activities, including non-financial activities. It may also be assigned to review compliance with laws, regulations and management policies and directives.

Note (a). The King III Report identifies the functions of internal audit as

* evaluating the company's governance processes including ethics
* performing objective assessments of the effectiveness of risk management and the internal control framework
* systematically analysing and evaluating business processes and associated controls

* providing a source of information regarding fraud, corruption, unethical behaviour and irregularities.

3. External auditor's objectives

The objectives of the external auditor are to determine whether

* ***the work of the internal audit function*** and/or
* ***direct assistance*** from internal auditors, can be used and if so in which areas and to what extent.

Note: ***"Using the work of the internal audit function"*** means using work which has been carried out by the internal audit department under its own direction, e.g. the external auditor may use a report on a risk assessment conducted and compiled by external audit. ***"Direct assistance"*** from internal auditors means the use of internal auditors to perform audit procedures under the direction, supervision and review of the external auditor.

4. External auditor's responsibility

It is important to remember that the sole responsibility for the audit opinion remains with the external auditor. Neither making use of the internal audit function's work, nor direct assistance from internal auditors, reduces the external auditor's responsibility for the audit opinion.

5. Evaluating the internal audit function

The first step in deciding on whether the work of the internal audit function can be used, will be for the external auditor to evaluate the internal audit function itself in respect of the objectivity and competence of the internal auditors and whether the internal audit function applies a systematic and disciplined approach, including quality control, to its work.

5.1 Objectivity of the internal auditors

Primarily the objectivity (the extent to which the internal auditors can act independently) will be determined by the following factors:

* the status of the internal audit function, i.e. is the department accorded a status or level of importance, authority and accountability which enables it, and its members, to be objective. In other words does its status support the function's ability to be free from bias, conflict of interest or undue influence to override professional judgements
* whether the internal audit function reports directly to those charged with governance e.g. the audit committee, and not to a functional manager such as the chief accountant
* whether the internal audit function is free of conflicting responsibilities e.g. members of the department are not drawn into "everyday accounting responsibilities and procedures"
* whether there are restrictions placed on the function by management e.g. denial of access to certain information, prohibiting communication with external audit
* whether those charged with governance (not management) oversee employment decisions relating to the internal auditors, e.g. appointment, dismissal, remuneration
* whether the internal auditors are members of a professional body which requires its members to adhere to the principle of objectivity.

5.2 Competence of the internal auditors

Competence of the internal audit function refers to the attainment and maintenance of knowledge and skills of the function as a whole, to enable assignments to be performed diligently and in accordance with applicable professional standards. The external auditor's determination of the internal auditor's competence will be influenced by whether the internal auditors

* have adequate training and proficiency in auditing
* have the required knowledge relating to financial reporting and the necessary industry specific knowledge to perform work related to the entity's financial statements
* possess a relevant professional qualification
* are members of a professional body which requires that they comply with professional standards including continuing professional development requirements
* are supported by adequate and appropriate resources necessary to perform their function
* are subject to sound policies with regard to hiring, training and assignment to internal audit engagements.

Note (a). Objectivity and competence must be viewed collectively and high levels of both are required. For example, internal auditors who are highly competent but are not able to be objective, are not much use to the external auditor!

5.3 A systematic and disciplined approach, including quality control

The external auditor must determine whether the internal audit function applies a systematic and disciplined approach to planning, performing, supervising, reviewing and documenting its activities. Factors which may affect the external auditor's evaluation include

* the existence and use of documented internal audit procedures or guidance covering such areas as risk assessment, work programmes, documentation and reporting
* whether the internal audit function has appropriate quality control procedures and policies in place which relate to leadership responsibilities within the function, ethical requirements, assignment performance, e.g. supervision and review etc.

Note (b). With regard to the objectivity, competence and discipline of internal audit, the King III Report makes the following recommendations/observations

* the internal audit function should adhere to the Institute of Internal Auditors' Standards for the Professional Practice of Internal Auditing and Code of Ethics
* the internal audit function should be independent from management. The board and management should defend and promote the independence of internal audit
* the head of internal audit should be designated as the Chief Audit Executive (CAE) or similar, to convey his status in the company
* the CAE should report functionally to the audit committee
* the CAE should have a standing invitation to all executive (or similar) committee meetings ***and*** should be given direct access to the chairman of the company
* the audit committee should ensure that the internal audit function is appropriately resourced and funded
* only properly qualified and experienced staff with high ethical standards should be appointed to internal audit
* the internal audit function should be seen as an integral part of the entity's assurance framework
* the CAE will set the tone of the internal audit function and should have (at least) the following attributes
  - strong leadership
  - respect for his competence and ethical standards
  - good communication skills.

6. Determining the nature and extent of work of the internal audit function that can be used

There is no magic formula which tells the external auditor exactly which work of the internal audit function can be relied upon and to what extent the work can be used. It is a matter of professional judgement which will be influenced by the following "principles"

* the external auditor must make all ***significant judgements*** in the audit engagement and therefore should perform more work directly (i.e. performed by the audit team) rather than using the work of the internal auditor. Significant judgements include
  - assessing the risks of material misstatements
  - evaluating the sufficiency of tests performed
  - evaluating significant accounting estimates
  - planning and performing relevant audit procedures.

Certainly the external auditor will consider information from, or work carried out by, the internal auditors pertaining to say, risk assessment, but will not rely to any great extent on this as a primary source of evidence. The external auditor must plan and perform an appropriate range of his own risk assessment procedures (one of which may be to review any internal audit risk assessment reports).

* the higher the assessed risk of material misstatement at assertion level, the greater the extent of work done directly by the external auditor
* the lower the objectivity and competence of the internal audit function, the greater the extent of work done directly by the external auditor. Exactly the same principle will apply where a risk of material misstatement is identified as a significant risk

* the external auditor must be satisfied that he has been sufficiently involved in the audit, particularly the gathering of sufficient appropriate evidence, to fulfil his sole responsibility for expressing the audit opinion.

Note. Examples of work of the internal audit function that can be used by the external auditor include
* testing of the operating effectiveness of controls
* substantive procedures involving limited judgement
* observations of inventory counts
* physical verification of existence of plant and equipment
* testing compliance with regulatory requirements.

7. Using the work of the internal audit function

7.1 Discussion and co-ordination with the internal audit function

The external auditor should discuss the planned use of the internal audit function's work with the internal auditors. This improves the efficiency of the audit and enables both parties to co-ordinate their activities. If the work to be used has yet to be performed, matters to be discussed may include, the nature, timing and extent of the audit procedures to be performed, any materiality considerations, methods of selecting items for testing, documentation to be produced, etc. If the work to be used has already been performed, the external auditor will need to plan the procedures he intends to conduct on the reports/documentation produced by internal audit.

7.2 Procedures to determine the adequacy of the work of internal audit

When the external auditor intends to make use of work conducted by internal audit, the external auditor should evaluate and perform audit procedures on that work, to confirm its adequacy for the external auditor's purposes

* The evaluation of work done by internal audit involves consideration of the adequacy of the scope of work conducted, and whether or not the evaluation of internal audit (see 5 above) remains appropriate. This evaluation may include consideration of whether or not:
  - the work has been performed by internal auditors who have adequate competence as internal auditors and the work was properly planned, performed, supervised, reviewed and documented, (similar to the external audit team evaluation)
  - sufficient, appropriate audit evidence has been obtained to be able to draw reasonable conclusions
  - conclusions reached are appropriate in the circumstances and any reports prepared are consistent with the results of the work performed, and
  - any exceptions or unusual matters disclosed by internal audit, are properly resolved.
* The nature, timing and extent of the audit procedures to be performed on the work of internal audit, will depend on the external auditor's judgement as to the risk of material misstatement and materiality of the area concerned, as well as the evaluation of internal audit. Such procedures may include examination of items already examined by internal audit, examination of other similar items and observation of internal audit procedures
* Evaluation of internal audit work would take place in a similar manner to the evaluation of the external audit team's performance, e.g. discussion with/enquiries of the personnel involved, review of working papers or completion of questionnaires
* The external auditor should record conclusions regarding the internal audit work that has been evaluated and tested in a workpaper to be kept in the audit file.

8. Determining whether, in which areas and to what extent, internal auditors can be used to provide direct assistance

8.1 Perhaps the major distinction between ***using the work of*** the internal audit function and the internal audit function providing ***direct assistance*** is the level of objectivity (independence) which the internal audit function has. Of course the competence of the internal auditors is important but in the evaluation of the internal audit function (see point 5 above), a little extra attention will be paid to the objectivity of the internal auditor. The external auditor will consider carefully

* the extent to which the internal audit function's organisational status and relevant policies and procedures support the objectivity of the internal auditors (see point 5)
* whether the internal auditor has any family or personal relationships with an individual working in, or responsible for, any aspect of the entity to which the (audit) work relates, e.g.

the external auditor would not obtain direct assistance from an internal auditor on work relating to accounts receivable if the internal auditor's spouse was the credit controller

* whether the internal auditor has any other association with the division or department to which the (audit) work relates
* whether the internal auditor has any financial interest in the entity other than remuneration on terms consistent with other employees at a similar level of seniority.

Note. The external auditor must be satisfied that the internal auditor has the ability to perform the proposed work without allowing bias, conflict of interest or undue influence of others to override professional judgements. It should be fairly obvious that the external auditor may not use internal audit to provide ***direct assistance*** if there are significant threats to the internal auditor's objectivity or if the internal auditor lacks the required level of competence.

8.2 As indicated in point 6 above, there is no magic formula for the external auditor to use in deciding on the nature and extent of the work that can be assigned to internal auditors providing ***direct assistance***. The following "principles" will be applied by the external auditor in making the decision

* the internal auditor must have the necessary competence to carry out the procedures properly and with an appropriate level of objectivity
* the external auditor must ***not*** use internal auditors to provide direct assistance to perform procedures that
  - involve making significant judgement
  - relate to situations where there is a high risk of material misstatement
  - relate to work with which the internal auditors have been involved (i.e. internal auditors cannot audit their own work)
  - relate to fraud risk (external auditors may make inquiries of internal auditors as a risk assessment procedure, but would not use internal audit to provide direct assistance when following up on a fraud risk)
* the extent of involvement (direct assistance) by internal auditors in the external audit, must not create the perception that the external audit lacks independence
* where there is an audit committee, the external auditor should communicate to the committee the nature and extent of the planned use of internal auditors to provide direct assistance. This is so that a "mutual understanding" that the use is not excessive, can be reached.

9. Using internal auditors to provide direct assistance

9.1 Bearing in mind that the internal auditors are employed by the client and not the external auditor, the external auditor should prior to using the internal auditors for direct assistance

* obtain written agreement from the client (CAE and/or audit committee) that the internal auditors will be allowed to follow the external auditor's instructions, and that the client will not intervene in the work the internal auditor performs for the external auditor
* obtain written agreement from the internal auditors, that they will
  - maintain confidentiality
  - inform the external auditor of any threats to their objectivity.

9.2 The external auditor must plan, direct, supervise and review the work performed by the internal auditors

* the nature, timing and extent of planning, directing, etc must take into account that the internal auditors are not independent of the client. Thus these procedures are likely to be
  - more extensive and
  - must include some checking back to underlying evidence by the external auditor
* during these activities (directing, supervising etc), the external auditor must be alert to any indications that the evaluation of the internal control function previously conducted (objectivity, competence, disciplined approach), is still appropriate.

10. Documentation

10.1 If the external auditor ***uses the work*** of the internal audit function, the following must be included in the audit documentation

- the evaluation of whether the function's organisational status and relevant policies and procedures, adequately support the objectivity of the internal auditors
- the evaluation of the level of competence of the function
- the evaluation of whether the function applies a systematic and disciplined approach including quality control
- the nature and extent of the work used and the basis for that decision
- the audit procedures performed by the external auditor to evaluate the adequacy of the work used.

10.2 If the external auditor uses internal auditors to provide ***direct assistance***, the following must be included in the audit documentation

- the evaluation of threats to the objectivity of the internal auditors and the level of competence of the internal auditors used in the direct assistance
- the basis for the decision regarding the nature and extent of the work performed by the internal auditors
- who reviewed the work and the date and extent of that review
- the written agreements obtained from the client (CAE or audit committee) and the internal auditors (confidentiality and threats to objectivity)
- the working papers prepared by the internal auditors who provided direct assistance.

ISA 620 - USING THE WORK OF AN AUDITOR'S EXPERT

1. Introduction

There are many instances where an auditor may find that he does not have the expertise required to obtain sufficient appropriate evidence pertaining to some aspect of the financial statements on which he is expressing an opinion. Such situations may include

- the valuation of complex financial instruments, land and buildings, plant and machinery, jewellery, works of art, intangible assets, etc
- actuarial calculations of liabilities relating to employment benefit plans
- estimation of mineral resources
- the valuation of environmental liabilities
- interpretation of contracts/laws
- tax compliance issues.

If such situations arise, the auditor will normally be obliged to engage an expert to assist in obtaining the evidence he requires, for example, a geologist (estimation of mineral reserves); an attorney (interpretation of a contract), or an actuarial scientist (used to provide pension fund information).

2. Definition of an auditor's expert

2.1 **"**Auditor's expert" means an individual or organisation possessing expertise (skills, knowledge and experience) in a particular field other than accounting and auditing, whose work in that field is used by the auditor to assist the auditor in obtaining sufficient appropriate evidence. An auditor's expert may be an auditor's ***internal*** expert, e.g. a partner or staff member in the auditor's firm, or an auditor's ***external*** expert, e.g. an independent geologist or attorney.

2.2 An auditor's expert must also be distinguished from a management's expert which is defined as an individual or organisation possessing expertise in a field other than accounting or auditing, whose work in that field is used by the client entity to assist the entity in preparing the financial statements, e.g. the ***client*** engages a property valuer to provide a fair value for the company's property.

3. Determining the need for an auditor's expert

3.1 The decision to make use of an auditor's expert will hinge around whether the auditor decides that it is not possible to obtain sufficient appropriate evidence without using the work of an expert.

3.2 An auditor's expert may be needed to assist the auditor in one or more of the following

- obtaining an understanding of the entity and its environment
- identifying and assessing the risks of material misstatement

* determining and implementing overall responses to assessed risks at financial statement level
* designing and performing further audit procedures to respond to assessed risks at the assertion level (further audit procedures)
* evaluating the sufficiency and appropriateness of audit evidence.

4. Determining the need to use an auditor's expert when management has used a management's expert in the preparation of the financial statements

Where management has used a management's expert, the auditor will need to determine whether he will need to engage an auditor's exert (to assist in obtaining sufficient appropriate evidence) or whether he can rely on the work of the management's expert. For example, BeeBop Ltd has a large portfolio of properties and management have engaged a property valuer to value the properties for financial year end reporting purposes. Bearing in mind that the valuer is ***not*** independent of the client, the external auditor will need to decide whether he can use the work of management's expert or whether he should engage his own expert to provide evidence pertaining to the valuation of the client's property portfolio. This decision will be based on such factors as

* the nature, scope and objectives of the management's expert's work, and how these align with the requirements of the external auditor
* the extent to which management was able to control or influence the work of the management's expert (independence)
* the management's expert's competence and capabilities
* whether the management's expert is subject to technical performance standards or other professional or industry requirements
* any controls within the entity over the management's expert's work.

Note. A management's expert could be an employee of the client or could be engaged by the client. Where the management's expert is an employee, the objectivity of the expert will be an even more important issue for the external auditor and a strong encouragement to engage his own expert.

5. Nature, timing and extent of audit procedures

The nature, timing and extent of procedures which the auditor must carry out in respect of the matters dealt with in 5.1 to 5.3 below, will vary depending on the circumstances of the audit. In determining the nature, timing and extent of procedures, the auditor will consider

* the nature (complexity and subjectivity) of the matter to which the expert's work relates, e.g. a difficult valuation of manufactured chemicals
* the risks of material misstatement in the matter to which the expert's work relates, e.g. high risk of overstatement of inventory due to inadequate allowance for chemical impairment
* the significance of the expert's work in the context of the audit, e.g. company holds significant quantities of inventory, the valuation of which is fundamental to fair presentation
* whether the expert is subject to the auditor's firm's quality control policies and procedures, e.g. if the auditor's expert is an external expert, he is not a member of the engagement team and therefore will not necessarily be subject to the quality control procedures adopted by the audit firm.

5.1 The competence, capabilities and objectivity of the auditor's expert

To be in a position to contemplate relying on the work of an auditor's expert, the auditor must be satisfied with the competence, capabilities and objectivity of the auditor's expert. This may be judged by

* having personal experience of the expert's "expertise"
* discussions with the expert
* discussions with other auditors who have experience of the expert
* obtaining knowledge of that expert's qualifications, membership of a professional body or industry association, licence to practice, etc
* knowledge of published papers or books by the expert
* whether the expert is subject to technical performance requirements such as ethical standards and other membership requirements of a professional body, accreditation standard or industry association
* the recognition that the expert is afforded by his peers and/or in the industry
* discussion with the expert as to his objectivity and independence in relation to the client e.g. financial interests in the client company or relationships with (relevant) client personnel,

(the auditor needs to establish whether there are any self interest threats, advocacy threats, familiarity threats, self review threats or intimidation threats, and if so whether there are adequate safeguards in place).

5.2 Obtaining an understanding of the field of expertise of the auditor's expert

The auditor is required to obtain a sufficient understanding of the expert's expertise to be in a position to

* determine the nature, scope and objectives of the expert's work
* evaluate the adequacy of the expert's work for the auditor's purposes

The auditor may already possess sufficient understanding from previous experience with the expert or from similar situations. If the auditor needs to acquire the knowledge, it can be obtained from such activities as discussion with the expert, attending professional development courses which are relevant, the internet and other searches of relevant databases, and discussion with other experienced auditors.

5.3 Agreement with the auditor's expert

The auditor must agree, normally in writing, on the following matters with the auditor's expert. Where the auditor's expert is an external expert, the agreement may be in the form of an engagement letter

* ***nature, scope and objectives***
  - the nature and scope of the procedures to be performed by the auditor's expert
  - the objectives of the auditor's expert's work in the context of materiality and risk considerations
  - any relevant technical performance standards or other professional or industry requirements the expert will be following, e.g. a specific valuation model
  - the assumptions and methods the expert will use
  - the effective date of the subject matter of the expert's work, e.g. financial year and inventory valuation.
* ***the respective roles and responsibilities of the auditor and the auditor's expert***
  - relevant auditing and accounting standards and relevant regulatory or legal requirements which must be complied with
  - the auditor's expert's consent to the auditor's intended use of the expert's report, including any reference to it or disclosure of the report
  - the nature and extent of the auditor's review/evaluation procedures
  - whether the auditor will test source data
  - the expert's access to the client's records and personnel
  - procedures for communication between auditor and expert
  - access to each party's working papers
  - ownership and control of work papers pertaining to the expert's work
  - the responsibility of the expert to perform the work with due skill and care
  - agreement on the expert's competence and capability to perform the work
  - any agreement for the auditor to inform the expert of the auditor's conclusions on the expert's work
  - the need for the expert to observe all ***confidentiality*** requirements.
* ***communication and reporting***
  - methods (written, oral) and frequency of communication (e.g. progress reports) and identification of the individual on the engagement team to whom the expert will report
  - deadline dates
  - the expert's responsibility to communicate promptly on
    - potential delays
    - potential reservations/limitations on the expert's findings
    - any restrictions imposed by the client on the expert
    - any circumstances that may create threats to the expert's objectivity.

6. Reference to the auditor's expert in the auditor's report

Where a standard audit report is given, no mention of the expert is necessary and no mention should be made. (Note: the use of an auditor's expert does not in any way reduce the responsibility of the auditor). If the auditor makes reference to the work of an auditor's expert in the auditor's report because such reference is relevant to understanding a modification to the auditor's opinion, the auditor must indicate in the report that such reference does not reduce the auditor's responsibility for that opinion.

CHAPTER 17

SUNDRY TOPICS

CONTENTS

Page

INITIAL AUDIT ENGAGEMENTS - OPENING BALANCES - ISA 510

1. Introduction 17/3
2. Auditor's objective 17/3
3. Procedures to be adopted 17/3
4. Reporting considerations 17/4

SUBSEQUENT EVENTS – ISA 560

1. Introduction 17/5
2. Applicable statements 17/5
3. Definitions 17/5
4. Types of subsequent event 17/6
5. Events occurring between the date of the financial statements and the date of the auditor's report 17/6
6. Facts which become known to the auditor after the date of the auditor's report but before the date the financial statements are issued 17/7
7. Facts which become known to the auditor after the financial statements have been issued 17/8
8. The decision on whether amendments are necessary 17/9
9. Action to prevent further reliance on the audit report 17/9

RELATED PARTIES – ISA 550

1. Introduction 17/11
2. Why the auditor is concerned about related party transactions 17/11
3. Definitions 17/11
4. Requirements 17/12

AUDIT DOCUMENTATION – ISA 230 & ISQC 1

1. Compliance with standards 17/13
2. General points and basic requirements 17/15

SPECIFIC TYPES OF AUDIT EVIDENCE

External confirmations – ISA 505 17/16

Enquiries regarding litigation and claims – SAAPS 4 17/17

External confirmations from financial institutions – SAAPS 6 17/19

Written representations – ISA 580 17/21

Analytical procedures – ISA 520 17/23

AUDIT CONSIDERATIONS RELATING TO AN ENTITY USING A SERVICE ORGANIZATION – ISA 402 17/25

INITIAL AUDIT ENGAGEMENTS - OPENING BALANCES - ISA 510

1. INTRODUCTION

ISA 510 establishes standards and provides guidance regarding opening balances where:

* financial statements for the prior period were not audited or
* where the financial statements for the prior period were audited by a predecessor auditor.

2. AUDITOR'S OBJECTIVE

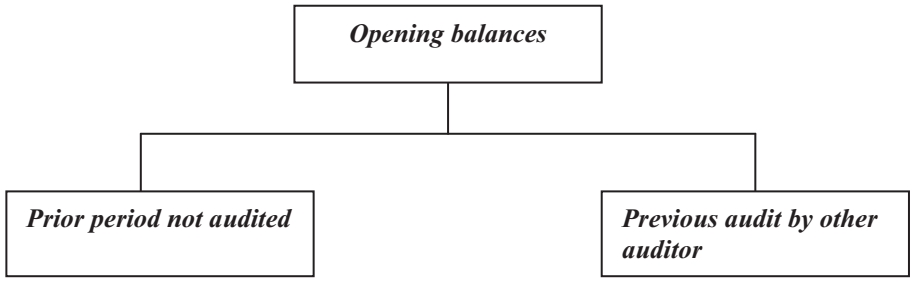
To obtain sufficient, appropriate evidence that:

* the opening balances do not contain misstatements that materially affect the current period's financial statements,
* appropriate accounting policies reflected in the opening balances have been consistently applied in the current period's financial statements, or changes in accounting policies have been properly accounted for and adequately presented and disclosed.

3. PROCEDURES TO BE ADOPTED

ISA 510 presents a very general approach to the audit procedures necessary with regard to opening balances. Where the previous year's audit was conducted by a predecessor auditor, the current auditor will normally have some access to prior year work papers and the predecessor auditor to refer to which should provide sufficient, appropriate evidence about the opening balances. Where the prior period was ***not*** audited, a "mini-audit" must in effect be conducted to obtain the necessary evidence about the opening balances for the current period.

The procedures to be adopted may vary for each situation, although the objectives remain the same. The diagram below illustrates this.



Prior period not audited

* Assess risk attached to each opening balance
* Consider significance of each opening balance
* Obtain understanding of accounting policies adopted and test for correct application and consistency
* Agree prior year closing balances through to current year opening balances
* Conduct common audit procedures on specific opening balances until reasonable assurance is obtained e.g.
  - test subsequent receipt of payments made by debtors
  - test subsequent payments made to creditors

Previous audit by other auditor

* Review predecessors audit work papers (NB Professional Conduct)
* Consider professional competence and independence of the predecessor auditor
* If not satisfied, revert to "prior period not audited" procedures.

- conduct analytical procedures
- carry out physical inspection e.g. inventory count and "roll back"

4. REPORTING CONSIDERATIONS

It is possible that the auditor is not satisfied with the opening balances and may believe that the audit report on the financial statements for the current year should be modified. The report can be modified based upon:

* ***the inability to obtain sufficient appropriate evidence*** relating to an opening balance.
  Example 1: The auditors were appointed half way through the current financial year and not having observed the physical counting of inventory at the end of the prior year, were unable to obtain sufficient evidence regarding the opening balance of inventory. If the ***possible*** effects of this were considered to be material but not pervasive, a qualified opinion "except for" would be appropriate. If the possible effects of this were considered to be material and pervasive, the auditor would issue a disclaimer of opinion. (Note: the qualification/disclaimer would relate to the statements of comprehensive income and cash flows, but not to the statement of financial position.)

* ***disagreement*** with an opening balance (see para 12 ISA 510).
  Example 2: The auditors were appointed half way through the current financial year. The financial statements had not been previously audited. The auditor is satisfied that the accounting policies applicable to certain opening balances had been incorrectly applied. The directors are not prepared to make adjustments. If the effect of the misstatements is material but not pervasive, a qualified opinion "except for" would be appropriate. If the effect of this was material and pervasive an adverse opinion would be issued (probably an unlikely situation!).

In the event of the above situations arising, the normal rules for modifying audit reports must be followed. See Chapter 18 and refer to ISA 700 and ISA 710.

SUBSEQUENT EVENTS – ISA 560

1. INTRODUCTION

Although the auditor reports on the financial statements as at the financial year end, audit evidence is not simply gathered up to that date and no further. When evaluating and concluding, the auditor is obliged to consider whether all material events occurring after the date of the financial statements and up to the date of the auditor's report, which may indicate the need for adjustment to, or disclosure in, the financial information on which the opinion is being issued, have been identified. ISA 560 - Subsequent Events takes this a step further by identifying not only the auditor's duty with regard to events occurring between the date of the financial statements and the date of the auditor's report, but also a duty should certain situations arise ***after*** the date of the auditor's report. (Note: the date of the auditor's report is the date on which the auditor signs the report.)

2. APPLICABLE STATEMENTS

There are two applicable statements; IAS 10 - Events after the Reporting Period, which defines and deals with the ***treatment*** of events after the reporting period, and ISA 560 - Subsequent Events, which covers the ***procedures*** to be adopted by the auditor with regard to events occurring subsequent to the date of the financial statements.

3. *DEFINITIONS*

3.1 ***Date of the financial statements*** – the date of the end of the latest period covered by the financial statements, normally the financial year-end date e.g. 30 June 0001

3.2 ***Date of approval of the financial statements*** – the date those with the recognized authority (normally the directors) assert that they have taken responsibility for the financial statements. (This is usually the date on which the directors sign the financial statements.)

3.3 ***Date of the auditor's report*** – the date the auditor selects to date the audit report on the financial statements. This date can only be when the auditor has obtained sufficient, appropriate evidence, including evidence that a complete set of financial statements have been prepared. This date ***cannot be before*** the directors have asserted that they have taken responsibility for the financial statements.

3.4 ***Date that the financial statements are issued*** – the date the auditor's report and audited financial statements are made available to third parties.

3.5 ***Subsequent events***
- events occurring between the date of the financial statements and the date of the auditor's report and
- facts that become known to the auditor after the date of the auditor's report.

Note (a): IAS 10 - Events after the Reporting Period, defines events after the reporting period as those events, both favourable and unfavourable, that occur between the end of the reporting period and the date when the financial statements are ***authorised for issue***.

Note (b): ISA 560 – Subsequent Events, deals with the time period between the date of the financial statements and the date of the auditor's report ***and*** splits the time period ***after*** the date of the auditor's report into two. The two time periods are:

(i) after the date of the auditor's report but before the date the financial statements are issued
(ii) after the financial statements have been issued to users.

The reason for this is that the auditor may react differently to facts that become known to him after the date of the auditor's report, depending on whether the financial statements have been issued or not.

4. TYPES OF SUBSEQUENT EVENT

4.1 Adjusting events

Events requiring ***adjustment*** in the financial statements. Adjustment must be made where the subsequent event provides evidence of conditions that ***existed*** at the end of the reporting period. IAS 10 states that in respect of such events "an entity shall adjust the amounts recognized in its financial statements to reflect adjusting events after the reporting period".

4.2 Non-adjusting events

These are events that are indicative of conditions that arose ***after*** the reporting period. If non-adjusting events after the reporting period are material, non-disclosure could influence the economic decisions of users taken on the basis of the financial statements. Accordingly the following should be disclosed:

* nature of the event
* estimate of the financial effect of the event or
* a statement that such an estimate cannot be made, if this is the case.

Many companies, particularly listed companies, will include further information about matters which might have arisen after the reporting period in the financial statements, simply to improve the quality of the statements and not specifically to comply with International Accounting Standards. The auditor's responsibility to this information is to satisfy himself that it does not contain misstatement of fact and that it is not misleading. (See Chapter 18).

4.3 Dividends

If a company declares a dividend after the reporting period, the entity shall ***not*** recognise those dividends as a liability at the date of the financial statements (end of the reporting period).

Dividends are usually approved at the AGM by the shareholders and therefore at the reporting date, the payment of the dividend is not a "present obligation".

4.4 Going concern

If management determines after the reporting date, that either

* it intends to liquidate the company or to cease trading
* or that they have no alternative but to do so, the financial statements ***may not*** be prepared on the going concern basis.

The reasoning for this is that if the company is no longer a going concern, the effect is so pervasive that a fundamental change in the basis of accounting is necessary. For example the company may have presented the financial statements on the going concern basis at 28 February 0001, on the grounds that management had a reasonable expectation that they would be awarded a large contract for which they had tendered. Appropriate disclosures would have been made. In the post reporting date period, the company was officially informed that it had ***not*** been awarded the contract. The company is no longer a going concern at reporting date although this fact was only confirmed after reporting date.

5. EVENTS OCCURRING BETWEEN THE DATE OF THE FINANCIAL STATEMENTS AND THE DATE OF THE AUDITOR'S REPORT

5.1 Duty of the auditor

Essentially the auditor has to do ***two*** things. Firstly, subsequent events must be ***identified*** and secondly, the ***treatment*** thereof in the financial statements must be audited to determine whether the treatment complies with IAS 10.

In terms of ISA 560, the auditor shall request management and, where appropriate, those charged with governance, to provide a written representation that all events occurring subsequent to the date of the financial statements which require adjustment or disclosure, have been adjusted for or disclosed.

5.2 Identification of subsequent events

The auditor should

* gain an understanding of, and review procedures adopted by management to identify subsequent events
* review minutes of meetings of directors, management, executive and audit committees held after the date of the financial statements
* obtain an update from client's legal representative on outstanding legal matters
* review the company's latest financial information
  - cash flow forecasts
  - budgets
  - monthly management reports
  - interim financial statements
* scrutinize (inspect) the financial records for the post reporting date period
* scrutinize (inspect) prior year work papers to identify types of events which have occurred previously
* obtain a management representation in respect of subsequent events
* make specific enquiries of management pertaining to
  - the status of items accounted for on tentative/preliminary/inconclusive data, e.g. bad debt allowance
  - new commitments/borrowings or guarantees
  - planned sale/disposal/abandonment of assets
  - realization/recoverability of assets at less than financial statement values
  - share issues, mergers, liquidations
  - assets destroyed, impaired or appropriated
  - developments in risk areas previously identified
  - unusual accounting adjustments which have been made or are contemplated
  - any event which may affect the appropriateness of accounting policies adopted at year-end
  - going concern ability of the company.

The intention of these enquiries is to gather the "latest" information about audit matters.

5.3 Auditing the treatment of the subsequent events

The auditor should:

* determine whether the subsequent event is an ***adjusting*** or ***non-adjusting*** event. The key issue is whether the event provides evidence of conditions that existed at reporting date; the client's interpretation cannot be relied upon without the auditor gathering sufficient appropriate evidence to support the client's interpretation
* evaluate the evidence supporting the subsequent event, e.g. notification from the liquidator of one of the company's major debtors
* reperform any casts or calculations which may be applicable to the event, e.g. it may be necessary to calculate an accrual for a decision based upon a legal judgment given after reporting date, which requires the backdating of a new set of pay rates
* where an adjustment must be made, determine by inspection, whether the adjustment has been correctly accounted for (i.e. the debits and credits are correct)
* where disclosure is required, inspect the notes for compliance with IAS 10:
  - nature
  - estimate of financial effect or
  - a statement that such an estimate cannot be made, if this is the case.

  Note: the "event" should be audited in terms of the assertions for "transactions and events" and/or "presentation and disclosure".

6. FACTS WHICH BECOME KNOWN TO THE AUDITOR AFTER THE DATE OF THE AUDITOR'S REPORT BUT BEFORE THE DATE THE FINANCIAL STATEMENTS ARE ISSUED

6.1 Duty of the auditor

There is ***no*** duty on the auditor to perform procedures to identify ***subsequent events after the date of the auditor's report***, ***but***, during this period if the auditor becomes aware of a fact which had it been known to the auditor at the date of the auditor's report, he should consider whether the fact

will affect the financial statements which have already been reported on, and if so whether the effect will (at least) be material. Essentially the auditor must decide on whether the audit report needs amendment, i.e. modification in some form.

6.2 Potential difficulties

If the effect of the fact is (at least) material, potential difficulties arise

* ***firstly*****,** a decision has to be taken by the directors on whether the financial statements should be ***amended***. The auditor has already decided that the matter is (at least) material, which implies that the decisions of users could be influenced, so ***theoretically***, the financial statements should be revised by adjustment or disclosure, and if they are not, the audit report should be qualified
* ***secondly***, the auditor's report and financial statements are likely to be under the control of the client (directors) as they have not yet been issued
* ***thirdly***, the manner in which the auditor proceeds if the financial statements require amendment, will depend upon ***management's willingness to amend*** the financial statements.

6.3 Management's attitude

If management is willing to amend the financial statements, the auditor should

* carry out the necessary audit procedures to confirm that the amendment (adjustment/disclosure) to the financial statements, is appropriate
* conduct further subsequent event procedures up to the date of the new auditor's report date
* provide management with a new audit report on the amended financial statements, correctly dated.

If management ***will not amend*** the financial statements, the auditor should

* redraft the report expressing a qualified or adverse opinion.

Note: This is only possible if the auditor has not yet released the (original) report to the client i.e. the auditor still has control over its distribution.

If the client has the original report and intends to release it with the incorrect financial statements, the auditor must inform the client that

* the financial statements including the audit report, should ***not*** be released
* and that if they are, the auditor will take steps to prevent reliance on the audit report.

7. FACTS WHICH BECOME KNOWN TO THE AUDITOR AFTER THE FINANCIAL STATEMENTS HAVE BEEN ISSUED

7.1 Duty of the auditor

* After the financial statements have been issued, the auditor has no obligation to carry out any audit procedures regarding these financial statements.
* However, if the auditor becomes aware of a fact which, had it been known at the date of the auditor's report, may have caused the auditor to amend the auditor's report, the auditor should discuss with management whether the financial statements need amendment (adjustment/disclosure) and if they do, inquire how management intends to address the matter.

7.2 Potential difficulties

* ***Firstly***, the financial statements have (already) been issued to a potentially wide audience
* ***Secondly***, the directors may not be prepared to do anything about it.

7.3 Management's attitude

* If management agree to amend the financial statements, the auditor's life will be a lot easier! The auditor will
  - carry out procedures to ensure the amendment is appropriately implemented (adjustment/disclosure)
  - conduct subsequent event procedures up to the date of the new auditor's report
  - issue a (new) revised audit report with an "emphasis of matter" or "other matter" paragraph which refers to a note which explains the revision and reissue of the report

- review the steps taken by management to notify users that the original financial statements issued, have been revised

* If management will not agree to issue revised financial statements (i.e. make the necessary adjustments/disclosures) or do not revise them adequately, or do not take suitable steps to notify those who are in receipt of the original (incorrect) financial statements, the auditor should
  - notify those charged with governance that action will be taken by the auditor to prevent reliance on the auditor's report.

8. THE DECISION ON WHETHER AMENDMENTS ARE NECESSARY

The auditor may experience some difficulty in deciding whether amendments to the financial statements are absolutely necessary, particularly where the directors are not willing to make amendments and the financial statements have already been issued. In making this decision, the auditor will consider the following:

* the reasons why the directors refuse to amend the financial statements, i.e. is there an intention to deceive users?
* the potential risk to which users may be exposed if they make decisions based on the original financial statements
* the severity of the effect on the auditor's report if the subsequent event or new fact is not dealt with, e.g. a ***material and pervasive*** qualification might be necessary
* the time elapsed since the audit report and subsequent management pronouncements. Audited financial statements are "old news" very quickly and are unlikely to be used in decision making for very long after issue
* the imminence of issue of the next year's audited financial statements. The matter could possibly be dealt with satisfactorily in these financial statements
* the practicality of communication with users; if for example, the financial statements have not been issued to users, a revised audit report could possibly be attached to them. If, however, the financial statements have been widely distributed, it will be far more difficult and ***possibly*** would not be cost effective to re-issue the financial statements
* any legal advice that the auditor may have sought.

***NOTE*:** The above considerations will be assessed cumulatively.

9. ACTION TO PREVENT FURTHER RELIANCE ON THE AUDIT REPORT

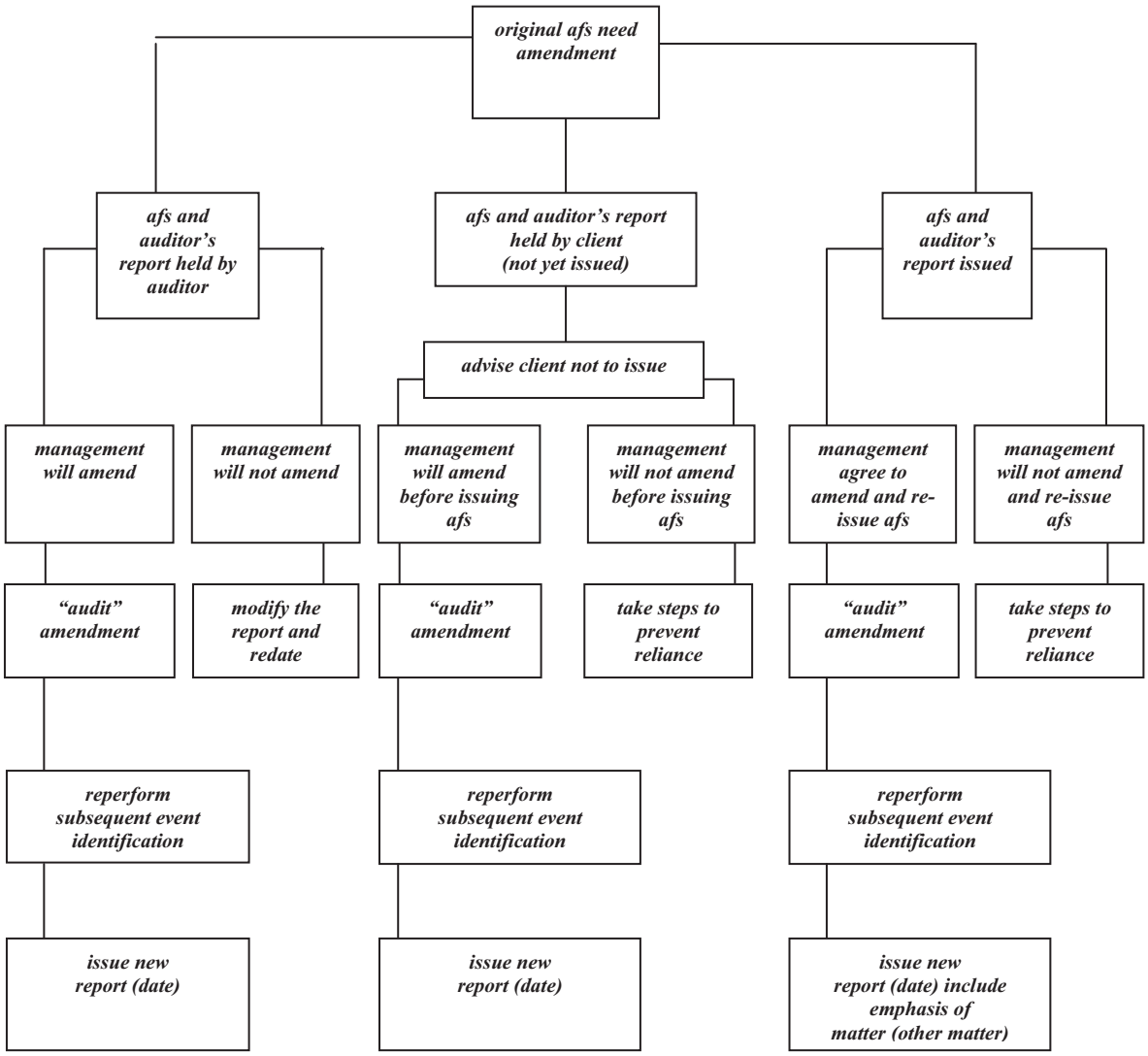
As can be seen from the diagram below, there are situations where the auditor needs to prevent reliance on the audit report. The following measures can be taken by the auditor to prevent reliance:

* make use of the auditor's right to address the shareholders at any general meeting, Companies Act 2008 Sec 93. This is of course, only possible if a general meeting is scheduled
* notifying each person whom the audit firm knows has received the financial statements, e.g. shareholders, or the client's bank
* making an announcement through the public media, e.g. financial publications. This is probably only appropriate for large companies
* notifying any regulatory agency which may have jurisdiction over the audit client, i.e. the JSE
* putting into action the recommendations of legal advisors who should be consulted prior to any action being taken.

When communicating with these individuals or entities (other than under Sec 93), confidentiality should be borne in mind. The notification should simply state that the audit report can no longer be relied upon. It is not appropriate to provide details of the matter in question. Any concerned user could then contact the directors for an explanation.

See appendix on following page which illustrates the amendment decision process.

Appendix – Responding to (original) financial statements which need amendment



RELATED PARTIES – ISA 550

1. INTRODUCTION

ISA 550 – Related Parties, places responsibilities on the auditor to perform audit procedures to identify, assess and respond to the risks of material misstatement arising from the entity's failure to appropriately account for or disclose related party relationships, transactions or balances in accordance with International Accounting Standards.

2. WHY THE AUDITOR IS CONCERNED ABOUT RELATED PARTY TRANSACTIONS

There are essentially two reasons that the auditor is interested in related party transactions

2.1 ***Inherent risk***: such transactions are ***inherently*** more risky because the transacting parties are not ***independent*** of each other.

* This may result in non-arms length transactions motivated by considerations other than sound business practice. Related party transactions may not be conducted under normal market terms and conditions. It should also be noted that this lack of independence will adversely affect the reliability of any evidence presented to the auditor by the related parties in support of any related transactions. Thus the risk of material misstatement going undetected is greater where related parties are involved.
* Related parties may operate through an extensive and complex network of relationships and structures which in turn may give rise to "difficult to audit" complex related party transactions.

2.2 ***Disclosure requirements***: there may be disclosure requirements in respect of the related party relationship or transaction; for example, loans by subsidiaries to holding companies. The auditor is required to ensure that relevant disclosure requirements are satisfied. IAS 24 – Related Party Disclosures.

2.3 ***Fraud:*** By gaining an understanding of the entity's related party relationships and transactions, the auditor is in a better position to evaluate the possibility of fraud occurring at a client arising from the presence of related parties. For obvious reasons fraud may be more easily committed through related parties.

3. DEFINITIONS

3.1 ***Arms length transaction*** – a transaction conducted on such terms and conditions as between a willing buyer and a willing seller who are unrelated and are acting independently of each other and pursuing their own best interests.

3.2 ***Related party***

- a person or entity that has control or significant influence, directly or indirectly through one or more intermediaries, over the reporting entity (i.e. the company whose financial statements are being audited).
- another entity over which the reporting entity has control or significant influence, directly or indirectly through one or more intermediaries.
- another entity that is under common control with the reporting entity through common controlling ownership, owners who are close family members or common key management.

In terms of ISA 550, ***control*** is the power to govern the financial and operating policies of an entity, and ***significant influence*** is the power to participate in the financial and operating policy decisions of an entity, but without control over those policies. Examples of situations where control or significant influence may be present

* direct or indirect equity holdings or other financial interests in the entity which is being audited, e.g. company A holds 55% of the shares in company B (company being audited)
* the entity which is being audited holds equity or other financial interests in other entities e.g. company P holds 40% of the shares in company Q and 60% of the shares in company R.
* being part of those charged with governance or key management e.g. the CEO controls the board (exerts significant influence)
* being a close family member of any person referred to in the point above, e.g. CEO's wife

* having a significant business relationship with the person who is part of governance or key management e.g. being a joint shareholder with the CEO in a private business venture.

It is submitted that the definition should not be taken too "technically"; from the audit perspective, the questions that must be asked are whether the transactions with related parties are motivated by ordinary business considerations, and correctly disclosed. Control and significant influence must be assessed realistically, regardless of preset levels or percentages. Has party A significantly influenced or controlled party B in respect of the transaction? It must be borne in mind, related party transactions are considered to be an ordinary feature of business and the vast majority are properly motivated and disclosed. However, the potential for misstatement is present and this risk must be addressed by the auditor.

3.3 ***Related party transactions -*** A transfer of resources, services or obligations between related parties regardless of whether a price is charged.

4. REQUIREMENTS

4.1 When performing risk assessment procedures and related activities in compliance with ISA 315 (Revised) (obtaining an understanding of the entity) and ISA 240 (responsibilities to fraud), the auditor must obtain an understanding of the entity's related party relationships and transactions

* inquire of management regarding the identity of the entity's related parties
* establish and understand the relationship between the entity and the related party e.g. close family relationship, equity, common business venture
* determine from management whether any transactions were entered into during the period under audit with related parties and if so, the nature and purpose thereof
* understand and evaluate the controls if any, that are in place at the entity to
  - identify, account for and disclose related party relationships and transactions
  - authorize and approve such transactions and
  - authorize and approve significant transactions outside the normal course of business (these may be related party transactions)
* enquire of others within the company as to the existence of related parties and related party transactions, e.g. internal audit, in-house legal counsel, risks and ethics committee members, audit committee.

4.2 In the discussions which are held with the engagement team, the susceptibility of the entity's financial statements to material misstatement due to fraud or error arising from the related party relationships and transactions should be specifically discussed, and the team should be provided with and share relevant information relating to related parties/transactions on an ongoing basis.

During the engagement team discussions on related parties, the following matters should be considered:

* the nature and extent of the entity's relationships and transactions with related parties
* the importance of maintaining professional scepticism throughout the audit regarding the potential for material misstatement associated with related parties
* the circumstances or conditions of the entity that may indicate the existence of related party relationships or transactions that management has not specifically identified or disclosed to the auditor (e.g. a complex organizational structure) and how they may be fraudulently exploited
* the records or documents that may indicate the existence of related party transactions, e.g. register of directors' interest in contracts, minutes of directors' meetings, lease agreements
* the manner in which related party transactions could be "hidden" by management, e.g. management override of controls and
* how transactions between the entity and related parties could be arranged to accommodate manipulation of the financial statements or misappropriation of assets.

4.3 During the course of the audit, the audit team must remain alert for evidence of the existence of related party relationships or transactions, that have not been previously identified or disclosed to the auditor. In particular, the audit team should:

* inspect bank and legal confirmations obtained for audit purposes

* inspect minutes of meetings of shareholders and those charged with governance
* inspect other relevant documents (see note 1 below)
* be alert to significant transactions outside the normal course of the entity's business and in doing so, establish the nature of the transaction and whether related parties could be involved (see note 2 below)
    - consider the business rationale (logic) of the transaction (arms length, designed to conceal misappropriation etc)
    - consider whether the terms of the transaction are consistent with the explanation for the (abnormal) transaction
    - consider whether the transaction has been appropriately accounted for and disclosed.

Note 1: Other documents or records which the auditor may inspect
- other third party confirmations
- income tax returns
- information supplied by the entity to regulatory authorities e.g. JSE
- declarations of conflict of interest from management or directors
- shareholders register
- life insurance policies (may be taken out on "key" personnel and may give light to a related party relationship)
- internal auditor's reports
- records of the company's investments.

Note 2: Transactions outside the normal course of business may include
- complex equity transactions such as mergers, restructuring, etc
- transactions with offshore entities operating in countries with weak corporate laws
- leasing of premises, rendering management services but no charge is levied
- sales made with unusually generous terms, e.g. large discounts, extended payment periods
- sales with a commitment to repurchase (circular arrangements).

4.4 The auditor must evaluate the accounting for and disclosure of identified related party relationships and transactions (IAS 24).

4.5 The auditor must obtain written representation from management, those charged with governance that
* they have disclosed to the auditor, the identity of the entity's related parties and all the related party relationships and transactions of which they are aware and
* have appropriately accounted for and disclosed such relationships and transactions.

4.6 The auditor must communicate with those charged with governance on any significant matters arising during the audit in connection with the entity's related parties.

4.7 The auditor must include in the audit documentation, the names of the identified related parties and nature of the related party relationships.

AUDIT DOCUMENTATION - ISA 230

1. COMPLIANCE WITH STANDARDS

There are two auditing statements (ISA 230 and ISQC 1) which are directly relevant to audit documentation commonly referred to as working papers.

ISA 230 requires:

1.1 That the auditor should prepare on a timely basis, audit documentation that provides
* ***a sufficient and appropriate record of the basis for the auditor's report, and***
* ***evidence that the audit was performed in accordance with International Standards on Auditing and applicable legal and regulatory requirements***.

The preparation of appropriate audit documentation enhances the quality of the audit and provides the auditor

with the means of proving that the audit was properly conducted should this be challenged, e.g. where the auditor is accused of negligence.

The audit documentation also

* assists the engagement team to plan and perform the audit
* facilitates direction, supervision and review on the audit in accordance with ISA 220 (quality control)
* makes members of the engagement team accountable i.e. their performance is reflected in their workpapers
* facilitates the audit quality control reviews of various kinds e.g. peer review by SAICA, partners from other firms etc, and external inspections if required
* provides a record of matters of continuing significance to future audits.

1.2 ***That an experienced auditor, having no previous connection with the audit, should be able to understand:***

* the nature, timing and extent of audit procedures performed to comply with ISAs
* the results of the audit procedures performed, and the audit evidence obtained
* significant matters and conclusions thereon.

1.3 ***That in documenting the nature, timing and extent of audit procedures, the auditor should record the identifying characteristics of the item/matters tested e.g.***

* document description and number (sales invoice number 2173)
* name of person who performed the work, date work was performed and the subject matter of enquiries
* journal entry numbers, dates, cycle
* starting point for samples and sampling intervals
* subject matter being observed. e.g. goods receiving activities.

A reviewer must be able to tie the workpaper to specific documents, dates, people, functions etc.

1.4 ***That significant matters identified on the audit must be documented, in particular***

* significant risks (and the audit response)
* results of audit procedures which indicate that the financial statements could be materially misstated, or which indicate the need to revise a previous assessment of material misstatement
* responses to risks
* circumstances that cause the auditor significant difficulty in applying the necessary audit procedures
* findings that could lead to modification of the auditor's report
* any departures from basic principles or essential procedures, e.g. ISAs, and reasons for the departure.

1.5 ***That the names of the preparer and reviewer and the dates on which they conducted their procedures, should be recorded on the work paper***.

ISQC 1 Quality control for firms that perform audits, requires:

1.6 That the firm must establish policies and procedures for ***engagement teams to put together finalised engagement files on a timely basis*** e.g. set deadlines, review and sign off files.

1.7 That the firm must establish policies and procedures ***designed to maintain confidentiality, safe custody, integrity (not allow tampering or contamination), accessibility and retrievability of engagement documentation***, e.g.

* use of passwords to access computerised workpapers
* back up routines
* controls over the distribution of workpapers e.g. sign a register
* physical controls over hardcopy and electronic work papers e.g. library routines, in a physically secure area.

1.8 That the firm must establish policies and procedures for ***the retention of engagement documentation***

for as long as they are needed by the firm, ensuring that the laws on retention of documents is adhered to.

2. GENERAL POINTS AND BASIC REQUIREMENTS

2.1 Audit documentation may be in various media e.g. written, digital, recorded.

2.2 Audit documentation is the property of the firm, and the firm is in no way obliged to make it available to the client or any other party, unless required to do so by law.

2.3 Workpapers should:

* be correctly headed regardless of their form e.g.
  Client : Knaves (Pty) Ltd Schedule No. FA1.
  Financial year end : 31 December 0001
  Date : 15 February 0002
  Section of Audit : Non-current Assets - Physical Verification
  Prepared By : Phil Collins
  Reviewed By : ..... Date .....,
* contain sufficient information concerning the matter to which the work paper relates, to enable the person reviewing the work paper, to judge whether the tests have been performed satisfactorily and to agree or disagree with the conclusion reached as a result of the tests,
* contain explanation and commentary on any unusual or exceptional matters and how they were dealt with,
* contain the ***conclusions*** of the ***preparer*** of the working paper,
* include adequate legends (keys) to symbols on the workpaper,
* display adequate cross referencing to other workpapers.

SPECIFIC TYPES OF AUDIT EVIDENCE

EXTERNAL CONFIRMATIONS – ISA 505

ISA 505 – External Confirmations, provides guidance on the principles relating to the auditor's procedure of obtaining external confirmations as part of the process of gathering sufficient appropriate evidence. ISA 505 is a general statement whereas SAAPS 4 – Enquiries regarding litigation and claims, and SAAPS 6 – External confirmations from financial institutions, are far more specific.

1. Introduction

In terms of ***ISA 500 – Audit evidence.***

1.1 Audit evidence is more reliable when it is obtained from independent sources outside the entity.

1.2 Audit evidence obtained directly by the auditor is more reliable than audit evidence obtained indirectly or by inference.

1.3 Audit evidence is more reliable when it exists in documentary form, whether paper or electronic.

Thus external confirmations provide potentially "good" (reliable) evidence, provided that the requirements set out below are satisfied.

2. Requirements

2.1 In terms of ***ISA 505,*** when carrying out external confirmation procedures, the auditor should

* maintain control over the process (not make use of the client to control the procedure)
* determine the information to be confirmed e.g. debtors balance at a particular date
* select the appropriate confirming party (e.g. must be an individual, competent and authorized to provide the confirmation)
* design the confirmation request to effectively obtain the evidence which is the objective of the confirmation request
* include specific instructions that the response details be sent direct to the auditor
* send (retain control over sending) the requests to the confirming party.

2.2 If the client refuses to allow the auditor to send a confirmation request

* the auditor should establish the reason for the refusal and seek evidence to support the validity and reasonableness of the client's explanation
* evaluate the implications of the refusal on his assessment of the risk of material misstatement including the risk of fraud
* perform alternative procedures to obtain sufficient appropriate audit evidence.

If the auditor concludes that the refusal is unreasonable, the auditor should communicate with those charged with governance.

If this does not succeed, the auditor will need to consider whether there has been a limitation of scope which affects the auditor's opinion. This will certainly be the case where alternative audit procedures cannot provide the necessary evidence.

2.3 If the auditor has doubts about the reliability of a response to a confirmation request, or no response is received (after following up), the auditor should consider

* the impact of this on his assessment of the risk of material misstatement (including the risk of fraud)
* perform alternative procedures to obtain the evidence and
* if the necessary evidence cannot be obtained, consider the implications on the audit opinion.

2.4 The auditor will evaluate the confirmations received to determine whether sufficient, reliable and relevant evidence has been obtained (usually as part of other evidence). It should be borne in mind that

* ***negative confirmations*** – i.e. confirmations which only request a response if there is a problem, are not particularly useful as the auditor does not know whether there is "no problem", or whether the confirming party did not receive the confirmation, or just didn't bother to respond, or whether the non-response was because there was an error but in favour of the confirming party!
* ***positive confirmations*** – i.e. confirmations which actually require the confirming party to respond whether they "agree" or "disagree", or to provide information, are far more valuable as they provide tangible and reasonably reliable evidence (assuring always that the basic requirements of external confirmations have been satisfied).

ENQUIRIES REGARDING LITIGATION AND CLAIMS – SAAPS 4

1. Introduction

Auditors frequently require information pertaining to the legal matters of their clients. For example, certain provisions arising out of legal matters may need to be recognized, or contingent liabilities may need to be disclosed.

SAAPS 4 requires that the auditor obtain sufficient, appropriate evidence regarding

* whether all material litigation and claims have been identified
* the probability of any material revenue or expense arising from such matters, and the estimated amount thereof and
* the adequacy of the accounting treatment of such matters, including their disclosure in the financial statements.

2. Management responsibility

It is the responsibility of management to adopt policies and procedures to identify, evaluate, record and report on all material litigation and claims.

3. Audit procedures to identify claims and litigation

To identify litigation and claims affecting the company, the auditor would perform the following audit procedures:

* review and discuss management's procedures for identifying and recording litigation and claims
* review and discuss management's procedures for identifying, controlling and recording legal expenses and associated revenues and expenses in appropriate accounts
* obtain and discuss with management:
  - a list of litigation and claims, including a description of the matters and an estimate of their likely financial consequences, and
  - an analysis of legal expenses
* review relevant documents, for example, correspondence with attorneys, and
* obtain written representation regarding the completeness of material outstanding litigation and claims from management
* examine contracts, loan agreements, leases, insurance policies and claims and other correspondence
* inspect minutes of meetings of the directors, the audit committee, shareholders and appropriate committees
* obtain information from bank confirmations concerning guarantees etc
* develop a knowledge of the essential characteristics of the entity's business operations, including an understanding of the potential involvement in litigation and claims, e.g. environmental hazards.

4. Requests for attorney's representation letter

Where material litigation and claims have been identified, the auditor should seek written representation from the company's attorneys. This written representation is designed to

* assist the auditor in evaluating the reasonableness of management's estimates and
* corroborate the completeness of the litigation and claims identified.

As with all 3rd party confirmations, the representation letter should be sent by the auditor (not management, although they prepare it) and the attorney should be requested to return it directly to the auditor. The request for the representation letter will be on the client's letterhead.

5. Contents of the client's request to the attorneys to provide a representation letter

The matters included in the letter are as follows:

* identification of the name, and the end of the reporting period, of the company(ies) to which the enquiry relates, e.g. the holding company and its subsidiaries and the year-end date
* a list ***prepared by management*** which names each company which is a party to material litigation or claims and describes the nature of such litigation and claims, the amount claimed and its status
* management's estimate of the financial exposure (inclusive of costs) for each litigation and claim in respect of which the attorney has been engaged by the company
* a request that the attorney advise whether the items are properly described and whether management's evaluations are reasonable
* a request for comment on those litigation matters and claims on which the attorney disagrees with management
* a request for a list of any other litigation and claims dealt with by the attorney in relation to the

company (completeness)

* an indication of the amount below which litigation and claims are not considered to be material for the purposes of the enquiry regarding litigation and claims. (These claims need not be considered when attorneys take the opportunity of bringing further litigation and claims, of which they are aware, to the attention of the auditor.)
* a request that the response address events as at, and subsequent to, the financial year-end of the company(ies) as close as possible to the expected date of the audit report, and
* a request that the nature of, and reasons for, any limitation on the response, be communicated.

6. Example of a schedule sent to the attorney with the letter (see above) requesting an "attorney's representation letter"

Name of Entity: Crackerjac (Pty) Ltd
Financial year-end : 28 February 0001

Litigation and Claims			
Name of entity (subsidiary or division)	Management's description of matter (including current status and amount claimed as well as attorney's reference if known)	Management's estimate of the financial exposure (inclusive of costs and disbursements)	Attorney's remarks
Crackerjac (Pty) Ltd	Attorney Ref C/341 Claim by former employee for unfair dismissal Damages of R1 000 000	No exposure. Claim by employee is groundless Legal costs R15 000	This is the first claim against the company of this nature and it is difficult to predict the outcome. Historically 70% of these cases result in a favourable outcome for the plaintiff with a settlement of 40% of the amount claimed

We confirm that we are acting for Crackerjac (Pty) Ltd in relation to the above-mentioned claim and that management's description and estimates of the amounts of the financial exposure (including costs and disbursements) which might arise in relation to those matters, are in our opinion, over optimistic as detailed above.

In addition to the above matters, we wish to bring to your attention the following litigation and claims exceeding R100 000 of which we are aware, in relation to the company.

Case reference C/914
A customer of Crackerjac (Pty) Ltd is suing the company for R150 000. The claim arises out of the customer having suffered a severe laceration to his leg whilst using a garden tool manufactured by Crackerjac (Pty) Ltd. We have advised the company to settle out of court for R50 000. We believe that this settlement would be accepted by the plaintiff. Legal costs amount to R10 000.

Attorneys: *Doogood and Deefend* Dated: 15 April 0001

EXTERNAL CONFIRMATIONS FROM FINANCIAL INSTITUTIONS – SAAPS 6

1. Introduction

1.1 Virtually every business entity has dealings with a financial institution. The relationship may be simple e.g. the entity has a single current account with a bank, or complex, e.g. the financial institution provides overdraft facilities, assists the entity with foreign transactions, provides letters of credit and makes loans to the entity. The bank may also assist with very complicated transactions such as financial futures, interest rate swaps, option contracts etc. In general terms, the more extensive and complicated the entity's dealings with the financial institution are, the greater the impact on the balances and disclosures in the financial statements will be. SAAPS 6 provides guidance to the auditor with regard to obtaining external confirmations from his client's bank (financial institution) which provide primarily corroborative evidence about the balances and disclosures reflected in the annual financial statements pertaining to the dealings between the client and the bank.

1.2 SAAPS 6 provides an illustrative external confirmation request which includes nine "Form Types". Form types relate to the category of information about which the auditor is seeking confirmation/information. The auditor will include only those "form types" in the confirmation request about which he seeks information.

Form Type		***Example***
1. Assets	:	(Positive) balance on the current account, or a 30 day call account.
2. Liabilities	:	(Negative) overdraft balance on the current account, or short term loan.
3. Securities	:	Securities pledged or otherwise encumbered.
4. Contingent liabilities and Guarantees	:	Bills receivable discounted but not yet paid.
5. Derivatives	:	Forward rate agreements, option contracts.
6. Bills	:	Total of bills held for collection.
7. Letters of Credit	:	Letters of credit relating to foreign suppliers.
8. Cash Management Systems	:	Details of accounts included in the cash management system.
9. Authorised transactions/Signatories list	:	EFT "Dongle" holders, cheque signatories.

SAICA recommends that the format of the illustrative confirmation request in SAAPS 6 be adopted by auditors.

2. Requirements

2.1 Theoretically an external confirmation from a financial institution should be regarded as reliable evidence because it is independent evidence from a reliable source. However, this will only be the case if the following basic requirements are followed:

* The request for the confirmation certificate should be made by the auditor to the financial institution.

- the necessary authority must be given to the financial institution by the audit client to furnish the information requested by the auditor.
- the certificate must be sent directly to the auditor at the auditor's address.
- the request must be sent to the financial institution timeously and
- must be sent to the appropriate individual at the institution (most entities will have an individual at the bank with whom they deal, or alternatively the bank will have a designated

person who deals with issuing certificates of this nature).

* Obtaining the external confirmation certificate must be properly planned.
  - the date by which the certificate is needed must be set.
  - the auditor must decide exactly what information he requires from the financial institution. This may range from a simple confirmation of an account balance at year end, to a request for extensive confirmation of information relating to complex transactions such as those identified in the introduction paragraph.
  - the information to be provided to the financial institution so that it can respond properly must be gathered. For example, if a confirmation of balance is required, the account number of the account must be included, or if the auditor is seeking confirmation about debt covenants pertaining to loans made by the financial institution to the client, the request must include the details which the auditor wants confirmed. It is not a matter of the auditor requesting the financial institution to supply all the information, the auditor supplies the information and the institution confirms if it is correct.
  - the validity of the authority given by the client to the financial institution must be confirmed.
  - the appropriate individual to whom the confirmation request must be sent must be identified.

3. Completeness of financial institution accounts

3.1 The financial institution is under no obligation to advise an auditor that it holds an account or has other arrangements that have not been listed in the certificate request from the auditor. In fact, SAAPS 6 states that financial institutions usually include a disclaimer in the certificate regarding the completeness of the entity's ″bank″ accounts included on the certificate supplied to the auditor.

3.2 If the auditor considers that there is a risk (which could result in material misstatement) that the financial institution account balances may be incomplete, he will respond to the risk by conducting further procedures. These procedures would concentrate on the inspection of documentation which relate to the entity's dealings with its financial institution. These procedures which would be carried out before the confirmation request is sent may include the following:

* Comparison of the list of financial institution accounts for the current year with the list at the end of the previous financial year (differences to be followed up).
* Inspection of directors' minutes for the year to determine whether e.g.
  - new financial institution accounts were opened.
  - any financial institution accounts were closed.
  - agreements or covenants were entered into by the entity with the financial institutions.
  - any arrangements relating to securities, guarantees, derivations etc, were undertaken.
  - changes were made to authorised account signatories.
* Inspection of significant contracts for confirmation that any related financial matters were conducted through financial institution accounts already listed.
* Obtaining management representation as to the completeness of financial institution accounts information which management has supplied.

4. Use of electronic confirmations

SAAPS 6 makes the point that electronic confirmations are acceptable but that, compared to confirmations in paper form received directly by the auditor, they do present additional risks relating to reliability, because the proof of source may be difficult to establish.

Similarly the auditor must be aware that, when sending a confirmation certificate request electronically, confidential information about the client's financial dealings is being transmitted and that the integrity of the transmission may be compromised. The auditor must therefore be satisfied that both transmission and receipt of electronic confirmations is secure before sending a request or accepting a response from a financial institution as reliable audit evidence. Such controls may include electronic digital signatures, encryption and procedures to verify website authenticity.

WRITTEN REPRESENTATIONS - ISA 580

1. Introduction

ISA 580 – Written representations, deals with the auditor's responsibility to obtain written representations from management and, where appropriate, those charged with governance in an audit of financial statements. Written representations can be an important part of the evidence gathered, but do not, in themselves, provide sufficient, appropriate evidence. They are corroborative in nature.

2. Objectives

The auditor's objectives in obtaining written representations are, in terms of ISA 580

2.1 To obtain a written representation from management that it (management) has fulfilled its responsibility for the preparation of the financial statements and for the completeness of the information provided to the auditor.

2.2 To support (corroborate) other audit evidence relevant to the financial statements or specific assertions in the financial statements.

3. Requirements

3.1 The auditor should request ***written*** representations from individuals in management who have relevant responsibilities and knowledge of the matters concerned

* those responsible for the preparation of the financial statements
* chief executive officer, chief financial officer.

In some instances, management may consult other parties to assist in making the written representation. These will be individuals who have assisted in the preparation of the financial statements by providing specialist knowledge e.g. in house actuaries, legal counsel or staff engineers.

3.2 The auditor must request management to specifically provide written representation that

* it (management) has fulfilled its responsibility for the preparation of the financial statements
* it has provided the auditor with all relevant information and access and
* all transactions have been recorded and are reflected in the financial statements.

In addition to the representations above, the auditor may consider it necessary to obtain other written representations about the financial statements. These may include representations about:

* whether the selection and application of accounting policies is appropriate
* whether there has been appropriate recognition, measurement, presentation and disclosure of the following in terms of IFRS or IFRS for SMEs
  - plans or intentions that may affect the carrying value of assets and liabilities, e.g. intentions to discontinue certain operations
  - liabilities, both actual and contingent, e.g. pending lawsuits
  - title to assets, liens, encumbrances and assets pledged as security e.g. agreements to buy back assets previously sold
  - aspects of laws, regulations and contractual agreements that may affect the financial statements e.g. unintentional foreign exchange contraventions, loans made to a director or related person in contravention of the Companies Act
  - related party transactions
  - subsequent events
  - intended changes to capital, e.g. capitalization issues, rights issues.

ISA 580 does not restrict the auditor in obtaining written representations and although these representations do not feature particularly high on the hierarchy of evidence, they do force management to commit themselves in writing and hopefully to focus their minds on what they are representing. In addition to the above, various ISAs require that the auditor obtain management representations pertaining to the topic of that ISA, e.g. ISA 240 (fraud).

3.3 If the auditor has doubt about the reliability of the written representations of management or the requested written representations are not provided, the auditor should

* discuss the matter with management
* re-evaluate the integrity and diligence of management (is this a deliberate attempt to mislead or

hide information?)

* consider whether this unreliability or refusal affects other audit evidence gained on the audit (both its reliability and sufficiency)
* extend testing (evidence gathering) if necessary
* consider the affect on the audit opinion.

Management should be quite prepared to make the necessary representations and the auditor should be sceptical (or suspicious) if management makes unreliable, incomplete representations or refuses to do so at all. However, management representations are corroborative in nature and do not stand on their own; unreliable representations or an absence of representations will not automatically result in a qualification or disclaimer of the audit opinion.

4. Conclusion

* To be of value, management representations should be:
  - written, not oral
  - corroborated by other evidence
  - reasonable and consistent in relation to other evidence obtained
  - given by members of the management team who are sufficiently well informed on the particular matter about which representations are being made
  - addressed to the auditor
  - contain specific information
  - appropriately dated (preferably the same as the auditor's report)
  - appropriately signed, e.g. senior executive officer.

ANALYTICAL PROCEDURES - ISA 520

1. Introduction

In terms of ISA 520, the term "analytical procedures" means evaluations of financial information through analysis of plausible relationships among both financial and non-financial data. Analytical procedures also encompass such investigation as is necessary, of identified fluctuations or relationships that are inconsistent with other relevant information, or that differ from expected values by a significant amount.

The second part of this description of analytical procedures is perhaps the most important. Extracting ratios or making comparisons does not in itself provide much useful information. The important part is the interpretation and follow up of inconsistent fluctuations and unexpected outcomes. For example, establishing that the gross profit percentage for the year has declined, compared to the prior year, is not in itself particularly useful. Establishing the reason and following up on the reasons is the important part of the procedure.

2. Nature of analytical procedures

2.1 Analytical procedures are ***substantive*** in nature. The major analytical procedure is the comparison of the entity's financial information with, for example:

* prior year period information
* budgets and forecasts
* similar industry information (industry averages)
* divisions/branches/cost centres within the entity.

2.2 The other major analytical procedure is the study of relationships

* among elements of financial information e.g. sales commissions and sales
* among elements of financial information that would be expected to conform to a predictable pattern, based on the entity's experience e.g. gross profit percentages
* between financial information and non-financial information e.g. payroll costs and number of employees.

3. Purpose of analytical procedures

3.1 Analytical procedures are used:

* as risk assessment procedures in obtaining an understanding of the entity and its environment and the risk of material misstatement.
* to substantiate an assertion when analytical procedures will be more efficient or effective than tests of detail, e.g. a comparison of wages, period to period, by department, may provide sufficient evidence as to the fair presentation of the wage expense.
* to provide corroborative evidence in the final review stage of an audit.

4. Analytical procedures as substantive procedures

When intending to use analytical procedures, the auditor will need to consider a number of factors before deciding that their use is appropriate.

4.1 Suitability of using substantive analytical procedures

The auditor must decide whether analytical procedures are appropriate for producing sufficient, appropriate evidence

* ***the assessment of the risk of material misstatement*** e.g. the higher this risk, the more likely it is that more tests of details will be appropriate
* ***the tests of detail already conducted (on the assertion)*** e.g. analytical procedures may provide good corroborative evidence where tests of detail have already been conducted.

4.2 The reliability of the data on which the analytical procedures will be conducted

There is no point in performing analytical procedures on unreliable data – this gives unreliable results! The auditor will consider

* ***the source of the data*** e.g. external evidence is better than internal evidence.
* ***comparability*** e.g. the auditor must compare "apples with apples" not "apples with oranges"; ratios in a wholesale business will not be comparable with the same ratios in a retail business
* ***nature and relevance*** e.g. if a budget is being used for comparison, is the budget a well prepared, thought out document or a "just going through the motions of putting a budget together" type budget?

* ***controls over preparation of the data*** e.g. poor control over validity, accuracy and completeness, results in unreliable data.

4.3 Whether the expectation is sufficiently precise to identify a material misstatement

The auditor needs to consider whether the results of the analytical procedures will be specific enough to identify material misstatement. If the analytical procedure gives only a general indication about whatever it is that the auditor is testing, it will not really be that worthwhile. If the result can be broken down further it will be far more useful. For example, the auditor wants to use analytical procedures when planning the audit of the occurrence of sales, i.e. whether there will be material misstatement arising out of the inclusion of fictitious sales

* a straight comparison of the current year sales against the prior year sales will not be very useful, ***but***
* if sales from the current and prior years can be broken down into sales by product, branch, salesperson, month, region, category or purchaser etc, the individual comparisons of the breakdowns becomes very useful.

The auditor will consider the following factors

* the availability of information, both financial and non-financial
* the extent into which the information can be broken down
* the inherent predictability of the information e.g. there is little point in conducting extensive analytical review on information which normally fluctuates and in no predictable /expected pattern.

4.4 Acceptable fluctuations from expectations

When the auditor performs analytical procedures, there are likely to be deviations from what is expected e.g. based on historical data, the auditor expects an increase of 10 days in the "days outstanding ratio" for debtors as a result of newly introduced credit terms. Ratio analysis reveals that the increase is actually 15 days. Does the auditor accept 15 days? What if it is 11 days or 6 days? There is no simple answer or magic cut-off point. The auditor will have to assess this piece of evidence in conjunction with other evidence or may reassess his expectations. Yet another example of the importance of professional judgment.

5. Investigating results of analytical procedures

As discussed in the introduction, the actual computation of ratios and trends is, in itself, of little value. The success of analytical procedures will depend upon how efficiently and effectively significant fluctuations and inconsistencies are ***identified*** and ***followed up***. In following up, the auditor will need to obtain corroboration of any explanations given by the client and may decide to perform additional audit procedures.

AUDIT CONSIDERATIONS RELATING TO AN ENTITY USING A SERVICE ORGANIZATION - ISA 402

1. Introduction

1.1 A company may make use of other entities to carry out functions which would otherwise be carried out by the company itself. For example, a company may have its payroll processed by a computer bureau, or may outsource its entire invoicing and debtor management to another entity. Entities which offer these kinds of service are referred to as service organizations in ISA 402.

1.2 When an audit client makes use of a service organization, it in effect, becomes part of the client's accounting system and related internal controls. In terms of ISA 315 (Revised) (Understanding the Entity), the auditor is required to obtain sufficient understanding of his ***audit client's internal control***, to be in a position to identify and assess the risks of material misstatement arising from weaknesses in that internal control system. By implication therefore, the auditor has to identify and evaluate the risks of misstatement arising from the use of the service organization.

2. ISA 402 requires that in obtaining an understanding of the audit client and its environment, the auditor should obtain an understanding of

* the nature of the services provided by the service organization
* the terms of the contract between the client and the service organization
* the extent to which the client's internal control interacts with the service organization
* the client's internal controls relevant to the service organization, e.g. controls over the flow of source data to the service organization, and how the risks of using a service organization are managed (e.g. the risk of a collapse of the service organization)
* the service organization's capability and financial strength
* any available information about the service organization's information system, general controls and application controls, including 3rd party reports on the service organization by internal auditors, other auditors or regulatory agencies.

The auditor of the client company making use of the service organization (termed the user auditor) may obtain the necessary information about the service organization by
* contacting the service organization for specific information
* visiting the service organization and performing procedures
* obtaining a type 1 or type 2 report.

3. Reports from the auditor (service auditor) of a service organization on its internal controls (Type 1 or Type 2).

3.1 A service organization is itself a business entity and will want to satisfy its customers that the business is well controlled, efficient and reliable. To this end, the service organization may make available to its customers, reports by auditors engaged by it (the service organization) to evaluate and report on its internal control. This report is potentially very useful to the customer's auditors (user auditor), but will depend on the type of evaluation and report which was conducted by the service organization's auditor. ISA 402 deals with two types of report :

Type 1 A report on the ***description*** and ***design*** of internal control, and
Type 2 A report on the ***description*** and ***design*** and ***operating effectiveness*** of the service organization's internal control.

3.2 The ***Type 1*** report will consist of
* a description of the service organization's internal control, and
* an opinion on whether
  - the description is accurate
  - the internal controls are suitably designed to achieve their stated objectives
  - the internal controls have been implemented.

The ***Type 2*** report will be the same as the ***Type 1*** report but will in addition contain
* information on whether the internal controls are ***operating effectively***, and

* details of the tests performed by the service auditor and the results thereof.

3.3 Obviously the ***Type 2*** report is more valuable to the (user) auditor, as it produces ***evidence*** about the ***effectiveness*** of internal controls at the service organization and hence will be helpful in the identification and assessment of material misstatement. The ***Type 1*** report is of some value in gaining an understanding of the client (using the service organization) but is limited as it produces no meaningful evidence.

3.4 Where the auditor chooses to rely on a ***Type 2*** report, it will be necessary to evaluate the 3rd party (e.g. the service organization's service auditor) which provided the report. Independence and competence of the service auditor would be particularly important.

3.5 It is also important that the auditor relying on the report considers whether the nature, timing and extent of the tests of controls conducted by the service auditor, provide sufficient, appropriate evidence. It is not just a matter of accepting the report at face value.

4. An auditor who relies on the report of a service auditor engaged by the service organization, should not make any reference to this fact in his report. The use of a service auditor does not alter the user auditor's responsibility to obtain sufficient, appropriate evidence to afford a reasonable basis to support his audit opinion.

CHAPTER 18

THE AUDIT REPORT

CONTENTS

	Page
INTRODUCTION	18/2
AUDITING STATEMENTS RELATING TO REPORTING	18/2
OBJECTIVES	18/2
STRUCTURE AND CONTENT OF THE UNMODIFIED AUDIT REPORT	18/3
WHY THE AUDITOR MIGHT NEED TO MODIFY THE AUDIT REPORT	18/5
CIRCUMSTANCES WHEN A MODIFICATION TO THE AUDITOR'S OPINION IS REQUIRED	18/6
MATERIAL AND MATERIAL AND PERVASIVE	18/7
TYPES OF MODIFIED OPINIONS	18/8
COMPILING A REPORT WHERE THE OPINION IS MODIFIED	18/9
EMPHASIS OF MATTER PARAGRAPHS AND OTHER MATTER PARAGRAPHS IN THE INDEPENDENT AUDITOR'S REPORT – ISA 706	18/12
DIAGRAMMATIC REPRESENTATION OF THE DECISION TO MODIFY THE AUDIT REPORT	18/14
THE EFFECT OF A REPORTABLE IRREGULARITY (SEC 45 – AUDITING PROFESSION ACT 2005) ON THE AUDIT REPORT	18/15
COMPARATIVE INFORMATION –CORRESPONDING FIGURES AND COMPARATIVE FINANCIAL STATEMENTS - ISA 710	18/16
THE AUDITOR'S RESPONSIBILITIES RELATING TO OTHER INFORMATION IN DOCUMENTS CONTAINING AUDITED FINANCIAL STATEMENTS - ISA 720	18/17

INTRODUCTION

The drafting and issuing of the audit report is the final stage in the audit process. In terms of ISA 200, the objective of the audit of financial statements is to enable the auditor to express an opinion on whether the financial statements are prepared, in all material respects, in accordance with the applicable financial reporting framework adopted by the entity e.g. IFRS. To express it more simply (and to echo the opinion paragraph in the audit report), the objective is ***"to express an opinion on whether the financial statements present fairly in all material respects, the financial position of the company at a specified date and its financial performance and cash flows for a specified period prior to that date, in accordance with International Financial Reporting Standards and the requirements of the Companies Act of South Africa"*** The audit report is the auditor's expression of this opinion.

THE AUDITING STATEMENTS RELATING TO REPORTING

Reporting the audit opinion on financial statements is governed by a number of International Standards on Auditing statements (ISAs). The ISAs are as follows:

1. ISA 700 – Forming an opinion and reporting on financial statements.

2. ISA 705 – Modifications to the opinion in the independent auditor's report.

3. ISA 706 – Emphasis of matter paragraphs and other matter paragraphs in the independent auditor's report.

4. ISA 710 – Comparative information - corresponding figures and comparative financial statements.

5. ISA 720 – The auditor's responsibilities relating to other information in documents containing audited financial statements.

In addition to the above, SAAP3 (revised) provides illustrative auditor's reports for different situations which may arise on audit, e.g. adverse opinion reports, disclaimers, etc. The ISAs provide the basic "rules" and framework for reporting internationally. The recommended wording applicable to audit reports for South African companies is as illustrated in SAAP3 (revised).

OBJECTIVES

1. In terms of ISA 700 the auditor's objectives are to
- form an opinion on the financial statements based on an evaluation of the conclusions drawn from the audit evidence obtained and
- to express ***clearly*** that opinion through a ***written*** report that also describes the basis of that opinion.

2. To be in a position to form the opinion, the auditor must conclude on whether he has obtained reasonable assurance as to whether the financial statements as a whole are free from material misstatement (arising from fraud or error). In drawing this conclusion the auditor must consider:
- whether sufficient appropriate audit evidence has been obtained
- whether uncorrected misstatements are material (individually or in aggregate)
- whether the financial statements are prepared in terms of an applicable reporting framework, e.g. IFRS or IFRS for SMEs
- whether significant accounting policies selected and applied have been adequately disclosed
- whether these accounting policies are consistent with the applicable financial reporting standards and are appropriate
- whether the accounting estimates are reasonable
- whether the information presented in the financial statements is relevant, reliable, comparable and understandable
- whether there is adequate disclosure to enable the intended users to understand the effect of material transactions and events on the information conveyed in the financial statements
- whether the terminology used in the financial statements is appropriate.

3. If the auditor ***concludes*** that the financial statements as a whole are not free from material misstatement ***or*** if the auditor is unable to obtain sufficient appropriate evidence to conclude that the financial statements as a whole are free from material misstatement, the auditor must ***modify*** the auditor's opinion in accordance with ISA 705.

STRUCTURE AND CONTENT OF THE UNMODIFIED AUDIT REPORT IN TERMS OF ISA 700 AND SAAPS 3 (Revised)

1. Structure

* title
* addressee
* introductory paragraph
* Directors' responsibility for the financial statements
* Auditor's responsibility
* Auditor's opinion
* other reports required by the Companies Act paragraph
* Signing off.

Note (a): the report must be in "writing" i.e. hardcopy or electronic. The auditor can't just give a verbal audit report at the AGM!

Note (b): the structure given above relates to unmodified audit reports. The report is modified in various situations e.g. where the audit opinion is qualified or an emphasis of matter is required, and in such situations additional paragraphs will be added as explained later in this chapter.

2. Content

INDEPENDENT AUDITOR'S REPORT (title)

TO THE SHAREHOLDERS OF COMAK LIMITED (addressee)
We have audited the financial statements of Comak Limited, set out on pages 15 to 40 which comprise the statement of financial position as at 31 March 0001, and the statement of comprehensive income, statement of changes in equity and statement of cash flows for the year then ended, and the notes comprising a summary of significant accounting policies and other explanatory information .

Note (c) : including the word "independent" in the title adds to the credibility of the audit report by emphasizing that the auditor is reporting as an individual who is independent of the company being reported on.

Note (d) : the audit report for a public company is addressed to the shareholders
: an audit of a private company which is required to be audited because of its public interest score or because its Memorandum of Incorporation requires it, will also be addressed to the shareholders.
: the audit report for a close corporation is addressed to the members. (In terms of the Companies Act 2008, some CCs must be audited).

Note (e) : the introductory paragraph must identify the entity whose financial statements have been audited, what is being reported on and must specify the date and period covered by the financial statements.

Director's Responsibility for the Financial Statements
The company's directors are responsible for the preparation and fair presentation of these financial statements in accordance with International Financial Reporting Standards and the requirements of the Companies Act of South Africa, and for such internal control as the directors determine is necessary to enable the preparation of financial statements that are free from material misstatements whether due to fraud or error.

Note (f): The inclusion of the above paragraph in the report is intended to emphasise (for users) that the directors are responsible for the financial statements and the underlying internal control system.

Auditor's responsibility
Our responsibility is to express an opinion on these financial statements based on our audit. We conducted our audit in accordance with International Standards on Auditing. Those standards require that we comply with ethical requirements and plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgement, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Note (g): This paragraph is intended to convey to the user what the audit is about in general terms as well as the responsibility of the auditor, e.g. assess risk, plan the audit, etc. It makes it clear that despite "considering" internal control ***no expression of opinion on its effectiveness*** is given.

Opinion
In our opinion, the financial statements present fairly, in all material respects the financial position of Comak Limited as at 31 March 0001, and of its financial performance and cash flows for the year then ended in accordance with International Financial Reporting Standards, and the requirements of the Companies Act of South Africa.

Note (h): Instead of using the wording "present fairly" ISA 700 allows the phrase "give a true and fair view" to be used. In South Africa the term "present fairly" is used.

Note (i): The opinion paragraph must also identify the financial reporting framework in terms of which the financial statements have been prepared, e.g. IFRS, IFRS for SMEs.

Other reports required by the Companies Act
As part of our audit of the financial statements for the year ended 31 March 0001, we have read the Directors' Report, the Audit Committee's Report and the Company Secretary's Certificate for the purpose of identifying whether there are material inconsistencies between these reports and the audited financial statements. These reports are the responsibility of the respective preparers.

Based on reading these reports, we have not identified material inconsistencies between these reports and the audited financial statements. However, we have not audited these reports and accordingly do not express an opinion of these reports.

Note (j): The requirement for this paragraph was introduced in the revised SAAPS 3 (November 2013). See point 7 on page 18/19 for an explanation.

Note (k): The reports referred to will vary depending on whether the company is public or private. For example a private company will not necessarily have an audit committee and therefore there will be no audit committee report included with the financial statements. Public companies are by law required to have an audit committee and a company secretary so the reports/certificate referred to in the paragraph will be included with the audited financial statements but do not form part of them.

In practice the report is closed off in various ways by different auditing firms. However, it is important that the name of the designated auditor (the individual responsible for the audit) appears as well as the date of the audit report and the auditor's address. The following examples of closing off are acceptable:

Tommy Tickett	*Deloitte*
Thomas T Tickett Registered Auditor 44 Montrose Manor Durban 15 May 0001	Deloitte Director: Reginald Reddy Registered Auditor 21 The Crescent Durban 15 May 0001

Note (l): The date of the audit report should be no earlier than the date on which the auditor obtains sufficient appropriate evidence on which to base the opinion on the financial statements. By implication this means that the auditor will have considered the effect of events and transactions on the financial statements up to the date of signing. Before signing, the auditor must ensure that a ***complete*** set of financial statements has been prepared and that the directors have signed the financial statements to acknowledge their responsibility for them.

WHY THE AUDITOR MIGHT NEED TO MODIFY THE AUDIT REPORT

Refer to the diagrammatic representation of the decision to modify the audit report on page 18/14.

There are ***two reasons*** that the auditor might need to modify the audit report.

1. Firstly, the auditor may need to ***modify his opinion,*** and secondly there may be ***information*** which the auditor needs to ***add to the report for the benefit of users*** but which does ***not*** affect his opinion.

2. The auditor will ***modify his opinion*** if

2.1 He has been unable to gather ***sufficient appropriate evidence*** to support an unmodified opinion or

2.2 Because there are ***uncorrected misstatements*** that are material and which therefore affect his opinion on fair presentation. In terms of ISA 705 the auditor can:

* ***qualify*** his opinion i.e. "the financial statements present fairly ***except for*** …"
* give an ***adverse*** opinion, i.e. "the financial statements ***do not*** fairly present …."
* give a ***disclaimer*** of opinion, i.e. "we do not express an opinion on whether the financial statements fairly present ……"

3. The auditor may need to ***add information to the report*** for the benefit of users. The auditor

3.1 can add an "***emphasis of matter***" paragraph to draw the users attention to information which is ***already in the financial statements*** but which the auditor considers to be very important to users.

3.2 may be required to add an "***other matter***" paragraph which is included when the auditor wishes to draw the users attention to something which is relevant to the users understanding of the audit, the auditor's responsibilities or the audit report itself. For example, the auditor may be required to convey to the user that he (the auditor) has other reporting responsibilities, such as Sec 45 of the Auditing Act 2005, which relates to reportable irregularities. Note that "other matter" paragraphs are different to the "other reports required by the Companies Act" paragraph.

CIRCUMSTANCES WHEN A MODIFICATION TO THE AUDITOR'S OPINION IS REQUIRED

As explained below, there are various circumstances where the auditor will be required to modify the audit opinion. In these circumstances it is very important for the auditor to consider the ***nature*** of the circumstance because the ***nature*** of the circumstance will directly affect the type of modified opinion the auditor gives and consequently the wording of the audit report.

In terms of ISA 705 the auditor must modify the ***audit opinion*** when:

1. He is unable to obtain sufficient appropriate evidence to conclude that the financial statements as a whole are free from material misstatement. The auditor's inability to obtain ***sufficient appropriate audit evidence*** can arise from

1.1 Circumstances beyond the control of the audit client

e.g. the client's accounting records were destroyed by fire and were not adequately backed up

e.g. ongoing physical danger; political unrest has prevented the auditor from visiting certain of the audit client's warehousing or manufacturing facilities to conduct audit procedures such as inventory counts.

1.2 Circumstances relating to the nature or timing of the auditor's work

e.g. the audit client is required to account for an associated company using the equity method, but the auditor is not able to obtain sufficient appropriate evidence about the associated company's financial information to evaluate whether the equity method has been appropriately applied. (Remember that the auditor does not have the right to demand evidence from the associated company.)

e.g. the timing of the auditor's appointment is such that the auditor is unable to observe the counting of physical inventories.

1.3 Limitations imposed on the auditor by the client's management

e.g. management refuses to give the auditor access to the accounting records relating to directors' emoluments

e.g. the board will not allow the auditor to review the minutes of directors' meetings.

2. He concludes that, based on the audit evidence obtained, the financial statements as a whole are not free from material misstatement (disagreement with management).

This situation arises when at the conclusion of the audit there is material uncorrected misstatement in the financial statements. Note that ISA 450 – Evaluations of Misstatements Identified during the Audit, defines a misstatement as a difference between the amount, classification, presentation or disclosure of a reported financial statement item, and the amount, classification, presentation or disclosure that is required for the item to be in accordance with the applicable financial reporting framework, e.g. IFRS.

Looked at another way, this situation arises when the auditor, based on the evidence gathered on the audit, disagrees with one or more representations (assertions) made by the directors in the financial statement being audited. Remember that the financial statements are the responsibility of the directors and that the auditor's responsibility is to determine whether the financial statements are fairly presented.

Material misstatement of the financial statements may arise in relation to:

2.1 The appropriateness of the selected accounting policies.

e.g. the audit client values its inventory at replacement cost instead of the lower of cost or net realizable value – inappropriate policy

e.g. the audit client has decided not to capitalize a major finance lease it entered into during the financial year – inappropriate policy.

2.2 The application of the selected accounting policy

e.g. the audit client has appropriately selected to capitalize a finance lease but has not ***applied*** the policy in terms of the applicable standard; the client has raised the asset in the plant and equipment account and long term liabilities account at the amount which the company would have paid for the asset had they purchased it for cash.

2.3 The appropriateness or adequacy of disclosures in the financial statements.

e.g. the disclosures pertaining to directors' emoluments have not been presented as required by IFRS and Sec 30 of the Companies Act 2008

e.g. a very important contingent liability arising from a court case has not been disclosed at all.

MATERIAL AND MATERIAL AND PERVASIVE

The second matter which the auditor considers, is the extent to which the financial statements are affected, or may possibly be affected by the matter which may give rise to modification of the auditor's opinion, i.e. will the effect be ***material*** or will it be ***material and pervasive***. Bear in mind that if the modification arises out of a difference (misstatement), the auditor can state clearly what the difference is and can quantify its effect on the financial statements. If the modification arises because the auditor was unable to obtain sufficient appropriate evidence, he can only judge the ***possible*** effect of the matter on the financial statements. He will not have the necessary evidence to quantify the effect.

As discussed in chapter 7, the auditor will have given considerable thought to materiality, both in planning and performing the audit and in considering final materiality (which should align with planning materiality) so he has a good indication of what is material both quantitatively and qualitatively. What the auditor has to do now is measure the full effect or possible effect of the matter on the financial statements. Think of it like this. The auditor's final materiality level is R100 000. This means that in the auditor's judgement, misstatement in the financial statements of say, R105 000 would have at least a material effect on the decisions users make based on the financial statements. But what about misstatement of R250 000 or more? The affect of misstatement of this size relative to his materiality limit, is likely to be material ***and*** pervasive. Measuring the effect of a disagreement is far easier than measuring the effect of a limitation of scope. In the case of a modification arising from a scope limitation the auditor will still need to judge how extensively the limitation affects the financial statements, but he does not have actual amounts to work with. For example, if the limitation relates only to evidence relating to long-term loans the auditor might consider the possible effect to be material only, but if the scope restriction spreads to long term loans, creditors, capitalized leases and profit figures, the auditor is likely to consider that the scope limitation "pervades" (spreads throughout) the financial statements as a whole. The auditor still does not have exact amounts to work with and will have to rely on his professional judgement to judge the pervasive effects. ISA 705 defines "pervasive effects" as those that in the auditor's judgement

* are not confined to specific elements, accounts or items in the financial statements or
* if they are so confined, represent a substantial proportion of the financial statements or
* in relation to disclosures, are fundamental to a user's understanding of the financial statements.

Some guidance was given in an earlier version of the reporting statement and although it is no longer "current" it is still helpful. In terms of the former statement

* a modification of the audit opinion arising from ***misstatement*** becomes material and pervasive when its impact on the financial statements is so great that ***fair presentation as a whole has been undermined and*** an "except for" qualification will not adequately convey the ***misleading or incomplete nature*** of the financial statements.
* a modification of the audit opinion arising from ***insufficient appropriate evidence*** (a scope limitation) should be regarded as material and pervasive if the effect of the limitation has resulted in the auditor being unable to obtain sufficient appropriate evidence to the extent that it is simply impossible to express any opinion.

TYPES OF MODIFIED OPINIONS

At this stage, the auditor will have classified the ***nature*** of each matter giving rise to modification and will have considered the extent of the effect (***pervasiveness***) of each matter, individually and collectively, on the financial statements. It is now time to match nature and effect to arrive at the appropriate opinion. ISA 705 provides the (slightly adapted) chart below to guide this procedure:

Nature of Matter Giving Rise to the Modification	***Auditor's Judgement about the Pervasiveness of the Effects or Possible Effects on the Financial Statements***	
	Material but Not Pervasive	***Material and Pervasive***
Financial statements are materially misstated	Qualified opinion (except for)	Adverse opinion
Inability to obtain sufficient, appropriate audit evidence (scope limitation)	Qualified opinion (except for)	Disclaimer of opinion

We can deduce from the chart that:

1. All material but ***not*** pervasive modifications will be ***except for*** qualifications (but as you will see in the next paragraph, the wording of the report will be slightly different for modifications arising out of material misstatements, and modifications arising out of the auditor's inability to obtain sufficient appropriate audit evidence).

2. Where the effect of a ***misstatement*** is material and pervasive, only an adverse opinion can be given. An adverse opinion is a clear statement that the financial statements ***do not*** fairly present.

3. Where the effect of a ***scope limitation*** is material and pervasive, only a disclaimer of opinion can be given. This is because the auditor is unable to form an opinion – he is not in a position to say that the financial statements are fairly presented or that they are not fairly presented as he does not have the necessary audit evidence to make the decision.

4. The audit opinion can be modified "except for" in respect of two different matters and the matters may be of different natures, e.g. in the auditor's opinion long-term liabilities may be misstated, and he may have had his scope limited in respect of the audit of accounts receivable. For "multiple" except for qualifications to be appropriate, neither matter on its own can be material and pervasive.

5. An adverse opinion cannot be mixed with a disclaimer of opinion – the auditor can't say in the same report that the financial statements do not fairly present and then say that he doesn't know if they fairly present!

6. Similarly an "except for" modification cannot be included in an adverse opinion or with a disclaimer of opinion even if the nature of the matters to which they relate are the same.

COMPILING A REPORT WHERE THE OPINION IS MODIFIED – STRUCTURE AND WORDING

1. ***Example***: In addition to selling products to its customers on credit, Millco (Pty) Ltd has opened a factory shop from which it sells its products for ***cash only***. As this is a new venture, the controls over cash sales are poor. The factory shop has been very successful and turnover has increased. Cash sales are reflected at about 10% of total turnover.

   Decision: ***Qualified opinion except for –*** insufficient appropriate evidence, (limitation of scope)
   This opinion is given when an unmodified opinion cannot be given due to a limitation of scope, but the effect of the limitation is not so material and pervasive that a disclaimer of opinion is necessary.

Paragraphs	***Changes in wording arising from modification of the opinion*** * no change means no change from unmodified report (see pg 18/3).
Title	No change
Introductory	No change
Directors' Responsibility	No change
Auditor's Responsibility	No change
Explanation This paragraph is headed, Basis for qualified opinion.	A clear and concise explanation of the limitation of scope is inserted above the opinion paragraph. e.g. "***During the year the company opened a factory shop selling on a cash only basis. As controls over cash were poor we were unable to satisfy ourselves as to the completeness of cash sales recorded"***
Opinion The paragraph is headed, Qualified opinion".	The opinion paragraph is amended to reflect the modified opinion i.e. **"*In our opinion, except for the possible effects of the matter described in the Basis for Qualified Opinion paragraph*,** the financial statements present fairly …"
Other reports Cosact	No change
Signing off	No change

2. ***Example***: Cheapshot (Pty) Ltd sells for cash only. As a result of breakdowns in internal control on numerous occasions during the year, the auditor was unable to gather sufficient appropriate evidence relating to the completeness and accuracy of the accounting records for cash sales.

   Decision: Disclaimer of opinion – insufficient appropriate evidence (limitation of scope)
   A disclaimer of opinion is given when the possible effect of a limitation of scope is so material and pervasive that the auditor is unable to express an opinion.

Paragraphs	***Changes in wording arising from modification of the opinion*** * No change means no change from modified report.
Title	No change
Introductory	The introductory paragraph is amended to reflect that the auditor has been unable to conduct a proper audit. Instead of opening the paragraph with "We have audited …", the words "We were engaged to audit…" are used.
Directors' Responsibility	No change

Auditor's Responsibility	The auditor's responsibility paragraph is shortened to read "Our responsibility is to express an opinion on these financial statements based on conducting our audit in accordance with International Standards on Auditing. Because of the matter discussed in the Basis of Disclaimer of Opinion paragraph, we were not able to obtain sufficient appropriate audit evidence to provide a basis for an audit opinion".
Explanation This paragraph is headed "Basis for disclaimer of opinion"	A clear and concise explanation of the limitation of scope is inserted, e.g. ***"The company sells only for cash. As a result of numerous breakdowns in the system of control over sales, there was no system of control over such sales on which we could rely for the purpose of our audit. There were no satisfactory procedures we could perform to obtain reasonable assurance that all sales were completely and accurately recorded."***
Opinion This paragraph is headed "Disclaimer of Opinion".	The opinion paragraph is then replaced with a disclaimer of opinion, i.e. **"*Because of the significance of the matter described in the Basis for Disclaimer of Opinion paragraph we have not been able to obtain sufficient appropriate audit evidence to provide a basis for an audit opinion. Accordingly we do not express an opinion on the financial statements*."**
Other reports Cosact	No change
Signing off	No change

3. ***Example***: Basix Ltd, a manufacturing company has decided that it will not capitalize a material finance lease relating to a piece of equipment, on the grounds that the company has not leased an asset before and does not intend doing so in the future.

   Decision: ***Qualified opinion except for*** – uncorrected misstatement (disagreement)
   This opinion is given when an unmodified opinion cannot be given due to a disagreement (with the directors about accounting policies selected, the method of their application or the adequacy of disclosures) which is not so material and pervasive as to require an adverse opinion. This is a misstatement arising out of the selection of an inappropriate policy for machinery which the company has leased. Disagreement with IAS 17 – Leases.

Paragraphs	***Changes in wording arising from modification of the opinion*** * No change means no change from modified report.
Title	No change
Introductory	No change
Directors' Responsibility	No change
Auditor's Responsibility	No change

Explanation This paragraph is headed "Basis for Qualified Opinion".	A clear and concise explanation of the disagreement is inserted e.g. ***"The company has excluded from property, plant and equipment and liabilities in the accompanying statement of financial position, a lease obligation that should be capitalized in order to conform with International Accounting Standard IAS 17 – Leases. If this lease obligation had been capitalized, property, plant and equipment would be increased by Rxxxx, long-term liabilities would be increased by Rxxxx, the current portion of long-term liabilities would be increased by Rxxx and retained earnings would be increased by Rxxx at 31 March 0001. Additionally net profit would be increased by Rxxxx for the year then ended.***
Opinion This paragraph is headed "Qualified Opinion".	The opinion paragraph is amended to read ***"In our opinion, except for the effects of the matter described in the Basis for Qualified Opinion paragraph the financial statements present fairly …."***
Other reports Cosact	No change
Signing off	No change

4. ***Example:*** Markks Construction Ltd has refused to recognise certain significant losses which are expected to arise on two of four long-term contracts which are currently in progress. Had these losses been recognized, the company's profits would have been severely reduced.

   Decision: adverse opinion - uncorrected misstatement (disagreement)
   This opinion is expressed when the effect of a disagreement is so material and pervasive to the financial statements that the auditor concludes that an except for modification of the report is not adequate to reflect the misleading or incomplete content which pervades the financial statements. This situation amounts to a misstatement arising from the inappropriate application of IAS 11 – Construction Contracts.

Paragraphs	***Changes in wording arising from modification of the opinion***
Title	No change
Introductory	No change
Directors' Responsibility	No change
Auditor's Responsibility	No change
Explanation This paragraph will be headed "Basis for Adverse Opinion".	A clear concise explanation paragraph will be inserted e.g. ***"Provision has not been made for losses expected to arise on certain significant long-term construction contracts currently in progress. A provision should be made for foreseeable losses on individual contracts in accordance with International Accounting Standards IAS 11-Construction Contracts. If losses had been so recognised the effect would have been to reduce the profit before tax, the contract work in progress and retained earnings at 31 March 0001 by Rxxx and profit for the year by Rxxx".***
Opinion This paragraph will be headed "Adverse opinion".	The opinion paragraph is amended to read ***"In our opinion, because of the effects of the matter discussed in the Basis for Adverse Opinion paragraph, the financial statements do not present fairly, in all respects, the financial position….".***
Other reports Cosact	No change
Signing off	No change

5. Additional points relating to structure and wording.

5.1 Where the opinion is modified except for, for more than one matter, an explanation paragraph will be included for each matter. If the ***nature*** of the matters giving rise to the modifications is different (i.e. one matter is based on misstatement and the other is based on a scope limitation) the two explanation paragraphs will need to be separately identified. This is because reference to each paragraph will have to be made in the opinion paragraph.

Example. Assume that the misstatement matter is explained in paragraph (a) and the scope limitation matter is explained in paragraph (b). The opinion paragraph will read "In our opinion, because of the effects of the matter described in the Basis for Qualification paragraph (a) and because of the ***possible*** effects of the matter discussed in the Basis for Qualification paragraph (b) the financial statements present fairly in all material respects…...

5.2 Theoretically a situation could arise where the effect of misstatements is, in itself, material and pervasive ***and*** the effect of a scope limitation is also in itself, material and pervasive. Obviously as mentioned earlier it is not possible to combine an adverse opinion and a disclaimer of opinion. What does the auditor do? There is no clear answer, but the adverse opinion is the stronger modification, because it is an actual opinion. The scope limitation could be raised in an "Other matter" paragraph after the opinion paragraph, but with very clear and precise wording which makes it clear that an adverse opinion has been given.

5.3 Where an "Emphasis of matter" or "Other matter" paragraph is added, it must be placed ***below*** the opinion paragraph.

5.4 If the audit report includes a report on other legal and regulatory requirements, the main body of the report will have the words, "Report on the Financial Statements" inserted below the addressee, and the words "Report on other legal and Regulatory Requirements" inserted after the opinion paragraph.

5.5 The most desirable audit opinion is an unmodified opinion, as this sends a positive message to users. It signifies that the financial information which they may use for decision making is fairly presented

* although misstatements etc, will already have been discussed with management at the time they were discovered, any proposed modifications should be discussed with the individuals responsible for the financial statements in order to give them the opportunity to provide ***further information*** or to ***amend*** the financial statements in a way which will enable the auditor to express an unmodified opinion. This may include discussion with the board and/or the audit committee
* where, after following these steps, the auditor still believes that a modification is necessary, careful consideration should be given to whether the lesser modification i.e. "except for" can be given instead of an adverse opinion or a disclaimer. In other words, the ***material/ material and pervasive*** decision should be revisited
* the above steps are taken with the intention of concluding a positive and constructive audit. However, it must be emphasised that the auditor ***must not compromise the reporting or other standards*** in an attempt to arrive at an unmodified opinion.

EMPHASIS OF MATTER PARAGRAPHS AND OTHER MATTER PARAGRAPHS IN THE INDEPENDENT AUDITOR'S REPORT – ISA 706

As we discussed earlier in this chapter, the ***audit report*** can be modified in a way which does ***not*** amount to a modification of the auditor's ***opinion***. ISA 706 permits additional communication in the auditor's report by the inclusion of an additional paragraph called either an "emphasis of matter" paragraph or "other matter" paragraph after the opinion paragraph.

1. Emphasis of matter

1.1 In terms of ISA 706 an ***emphasis of matter*** is a paragraph included in the audit report that refers to a matter which is (already) ***appropriately presented or disclosed*** in the financial statements ***but*** which is, in the auditor's judgement, of such importance that it is fundamental to the user's understanding of the financial statements. Note that

* an emphasis of matter relates to a matter adequately dealt with in the financial statements
* an emphasis of matter is ***not a substitute*** for any type of modification of the auditor's opinion which may be required i.e. the auditor cannot replace an except for, adverse or disclaimer of opinion with an emphasis of matter.

1.2 Examples of where the use of an emphasis of matter paragraph may be appropriate

* the company has a going concern problem which has been adequately disclosed in the financial statements.
* the client company is involved in litigation, the outcome of which may materially affect the financial statements. The matter has been adequately disclosed and is very important.

Note (a): As indicated earlier in the chapter, where there are additional legal or regulatory reporting requirements an additional paragraph headed "Report on Other Legal or Regulatory Requirements" must be included. This will ***not*** be an emphasis of matter paragraph.

1.3. Where an emphasis of matter paragraph is to be included in the audit report it will

* be positioned beneath the opinion paragraph
* be headed up with a phrase which conveys the nature of the matter being emphasised e.g. "***Significant uncertainty regarding litigation"***.
* open with the words "***without qualifying our opinion above..."*** and be followed by a clear and concise explanation of the matter.

2. Other matter paragraphs

In terms of ISA 706 an ***other matter*** paragraph is a paragraph included in the auditor's report that refers to a matter ***other*** than those presented or disclosed in the financial statements, that in the auditor's judgement is relevant to the user's understanding of the audit, the auditor's responsibilities or the auditor's report. Note that

2.1 An "other matter" paragraph relates to a matter which does not need to be, and has not been dealt with or presented in the financial statements.

2.2 An "other matter" paragraph is ***not*** a substitute for any type of modification of opinion which may be required.

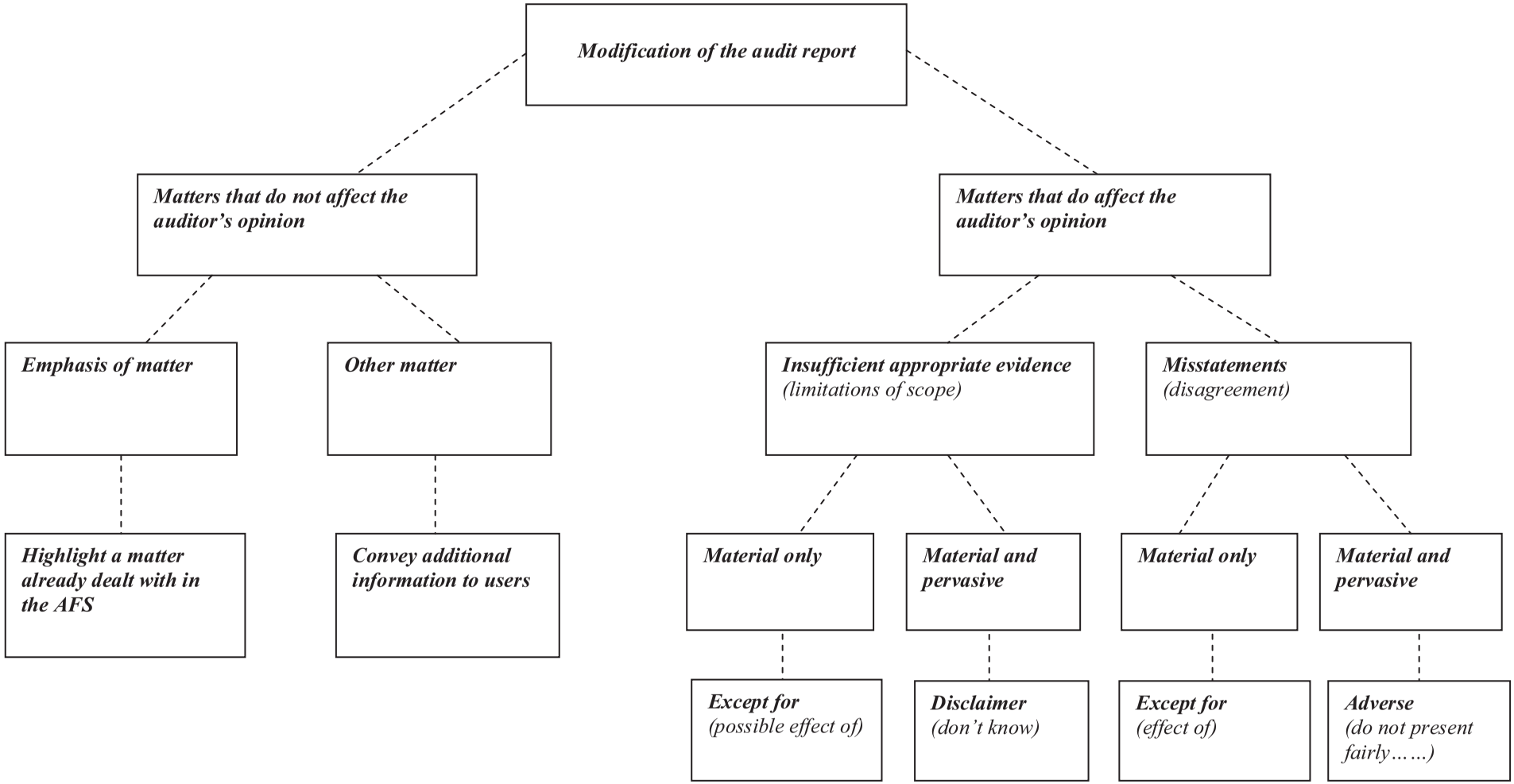
2.3 Like emphasis of matter paragraphs, "other matter" paragraphs are not that common. An example of where an "other matter" paragraph may be appropriate will be

* where there is a material inconsistency in "other information" included in a document containing audited financial statements e.g. the Chairman's Report in the annual report, is inconsistent with the financial statements and the directors refuse to have the inconsistency removed
* where there is a reportable irregularity
* where the prior year comparative figures were not audited.

2.4 When an "other matter" paragraph is to be included in the audit report it will

* be positioned beneath the opinion paragraph
* be headed up with a phrase which conveys the nature of the other matter
* if clarity is required, open with the words "***without qualifying our opinion above***" and be followed by a clear and concise explanation of the matter.

DIAGRAMMATIC REPRESENTATION OF THE DECISION TO MODIFY THE AUDIT REPORT



THE EFFECT OF A REPORTABLE IRREGULARITY (SEC 45 – AUDITING PROFESSION ACT 2005) ON THE AUDIT REPORT

1. Sec 44 of the AP Act states that the registered auditor ***may not, without qualification*** (modification) express an opinion to the effect that the financial statements

* fairly present in all material respects, and
* are properly prepared in terms of the financial reporting standards ***unless***
* the registered auditor has ***not*** reported a reportable irregularity to the IRBA ***or***
* if such report was sent, the auditor has been able, prior to expressing the audit opinion, to send a notification to the IRBA that he has become satisfied that no reportable irregularity has taken place or is taking place.

2. There are 3 possible situations which may give rise to the need for a reportable irregularity to be dealt with in the audit report.

Possibility 1. A reportable irregularity ***did exist***. It is no longer taking place, and adequate steps have been taken for the prevention or recovery of any loss as a result therefrom.

Possibility 2. A reportable irregularity exists i.e. it is continuing.

Possibility 3. The reporting process to IRBA is incomplete, i.e. the initial report alleging the existence of a reportable irregularity has been submitted by the auditor to IRBA, but the auditor has not submitted the second report confirming or withdrawing the allegation (30 days).

Perhaps the easiest way to convey what can be a very difficult reporting duty, is to describe the matter giving rise to the reportable irregularity and to consider the auditor's options. Assume that the first report has been made to the IRBA and management has been notified.

Example: Inbound (Pty) Ltd imports goods into South Africa. The auditor has reason to believe that during the past financial year the directors have been defrauding SARS by not declaring the true nature of the goods imported, thereby paying less import duties than are due.

Situation 1. The directors acknowledge the fraud, make full declaration to SARS, and make the necessary adjustments (e.g. raise SARS as a creditor) and make full disclosure in the financial statements. The auditor is satisfied.

Outcome 1. The auditor is able to notify the IRBA (second report) that the reportable irregularity ***did exist*** but has been resolved.

The audit report does not need qualification (as the financial statements are fairly presented) ***but*** must be amended by the inclusion below the opinion paragraph, of an additional paragraph headed "Report on Other Legal and Regulatory Requirements". ***"In accordance with our responsibilities in terms of section 44(2) and 44(3) of the Auditing Profession Act, we report that we have identified certain unlawful acts committed by the directors of Inbound (Pty) Ltd which constitute reportable irregularities in terms of the Auditing Profession Act, and have reported such matters to the Independent Regulatory Board for Auditors. The matters pertaining to the reportable irregularities have been described in note 7 to the financial statements".***

The directors have responded to the circumstances and conduct in question to the extent that we believe no further loss will be suffered by the parties identified in note 7 and that all amounts owed including penalties have been accounted for. The unlawful act described in note 7 is to the best of our knowledge no longer occurring.

Situation 2. The directors provide sufficient appropriate evidence to satisfy the auditor that no fraud has taken place.

Outcome 2. The auditor must notify the IRBA (second report) that no reportable irregularity existed.

The matter will have no effect on the audit report, i.e. no modification or additional paragraphs required because no reportable irregularity actually existed.

Situation 3. The directors acknowledge that the fraud has taken place, agree to discontinue the fraud but refuse to make any adjustments or disclosures to the financial statements or to notify the SARS.

Outcome 3. The auditor must notify the IRBA that the reportable irregularity did exist and as the directors will not take any corrective action, is continuing.

The audit report does need modification as the financial statements do not fairly present (no disclosure, no adjustment). The qualification will be based on disagreement (misstatement) and the auditor will need to judge whether it is material or material and pervasive.

In the basis of qualification paragraph the auditor will disclose information on the reportable irregularity. In addition the audit report must be amended by the inclusion of an additional paragraph headed:

"Report on Other Legal and Regulatory Requirements"
In accordance with our responsibilities in terms of section 44(2) and 44(3) of the Auditing Profession Act, we report that we have identified certain unlawful acts committed by the directors of Inbound (Pty) Ltd which constitute reportable irregularities in terms of the Auditing Profession Act, and have reported such matters to the Independent Regulatory Board for Auditors. We have also submitted the additional report to the Independent Regulatory Board for Auditors in terms of section 45(3) indicating that, in our opinion the reportable irregularity is continuing. The matters pertaining to the reportable irregularities have been described in the audit report above.

Situation 4. Although having communicated to the directors that a first report has been made to the IRBA, no response has been forthcoming from the directors.

Outcome 4. If the 30 day period for response has elapsed, the auditor has no option but to report to IRBA that the reportable irregularity exists. The auditor has no reason or evidence to change his original opinion. The effect on the audit report will be the same as for situation 3 i.e. modification of the opinion based on misstatement relating to disclosure in the financial statements, and the inclusion of the additional, "Report on other legal and regulatory requirements" paragraph.

Note: In the unlikely event that the auditor has to sign the audit report between sending the first report to the IRBA and the 30 day response date, (***possibility 3***) and the reportable irregularity has not been addressed, the auditor would have to include the details in the "Other Legal and Regulatory Requirements" paragraph but would need to convey that the 30 day response period had not expired at the date of the audit report. A far more desirable outcome would be to delay the audit report until the 30 day period for response has expired so that the appropriate report can be given.

ISA 710 – COMPARATIVE INFORMATION – CORRESPONDING FIGURES AND COMPARATIVE FINANCIAL STATEMENTS.

1. Introduction

This statement provides guidance on the auditor's responsibility for comparative information presented in the financial statements on which the auditor is reporting. In South Africa comparatives are presented as corresponding figures as part of the current period financial statements and are intended to be read in relation to amounts and disclosures relating to the current period.

2. Objectives and procedures

The auditor's objective with regard to the corresponding figures is to obtain sufficient appropriate evidence that the figures meet the requirements of the reporting framework adopted for the financial statements. This amounts to carrying out procedures to determine whether:

* corresponding figures agree with the amounts and other disclosures presented in the prior

period or, when appropriate, have been properly restated and

* accounting policies used for corresponding figures are consistent with those applied in the current period or if there have been changes in accounting policies, these changes have been properly accounted for and adequately presented and disclosed.

Where the audit engagement is ongoing, the above requirements should be easily achieved by reference to the auditor's prior year working papers and the prior year financial statements. In the situation where the prior period financial statements were either audited by another auditor, or not audited at all, the guidance given in Chapter 17 - ISA 510, Initial Audit Engagements - Opening Balances will need to be followed. In effect, a "mini-audit" on the opening balances will be conducted.

Where the auditor becomes aware of a possible misstatement in a corresponding figure when performing the current period audit, additional appropriate procedures must be conducted to establish the nature and extent of the misstatement. Its effect on fair presentation of the corresponding figures as well as the current period figures can then be assessed.

3. Reporting

Ordinarily the audit report will make no mention of comparatives. Because South Africa adopts the corresponding figure method of presenting comparatives, it is implied that the auditor's opinion is on the financial statements as a whole, including the corresponding figures.

* when the auditor's report on the prior year financial statements included a modified opinion and the matter giving rise to the modification, has been properly ***resolved*** and accounted for, the current audit report need not refer to the previous modification

* when the auditor's report on the prior period included a modified opinion and the matter which gave rise to the modification is ***unresolved*** the auditor will modify the current audit opinion ***if*** the unresolved matter affects the current year's audit opinion evaluated in terms of the normal modification procedures

* when the auditor discovers, whilst performing the current period audit, a material misstatement that affects the prior period's financial statements on which an unmodified opinion was given, it would amount to a subsequent event and should be treated in terms of the guidance in ISA 560 –Subsequent Events, which is dealt with in Chapter 17

* an "other matter" paragraph should be added where applicable, for example
  - the financial statements of the prior period were audited by the predecessor auditor or
  - were not audited at all.

ISA 720 – THE AUDITOR'S RESPONSIBILITIES RELATING TO OTHER INFORMATION IN DOCUMENTS CONTAINING AUDITED FINANCIAL STATEMENTS.

1. Introduction

Annual financial statements are usually issued in what is termed the "annual report or more recently the integrated report". Besides the financial statements the annual report/integrated report will include other information such as the chairman's report, the report on corporate governance, reports on sustainability, various reports on operations, lists of directors etc. The auditor's responsibility is to give an opinion on the annual financial statements ***as described*** in the Companies Act 2008 Sec 29. This definition does not include "other information". Therefore the auditor has no responsibility to give an opinion on "other information" and would not be in a position to do so unless engaged by the client to perform an audit of such information (which in itself may not be possible).

2. *The auditor's objective and duty to other information*

The objective of the auditor is to respond appropriately when the audited financial statements include other information that could undermine the credibility of those financial statements and the audit report. The auditor has a duty to read the other information with the intention of identifying ***material inconsistencies*** (contradictions) between the other information and the financial statements. The reason that this duty arises, is because if such material inconsistencies appear in the published annual report, a user may be confused, and doubts may be raised about the auditor's opinion.

On reading the other information contained in the annual report the auditor may also become aware of an apparent ***material misstatement of fact*** in the "other information". Material misstatements of fact relate to matters ***which do not*** appear in the financial statements and therefore cannot be regarded as "inconsistencies".

3. *Examples of inconsistencies*

* The Chairman's Report suggests a far more favourable financial position than is reflected by the annual financial statements.

* The Operations Director's Report on a discontinuation of part of the company's operations reflects a loss on discontinuation materially less than that reflected in the financial statements.

* The same report contains a paragraph which raises the probability of technical obsolescence of the company's products, a factor which was not taken into account when impairment losses for inventory were considered.

4. *Action required by the auditor: material inconsistencies*

* The auditor must determine whether the material inconsistency requires an amendment of the ***financial statements*** or the ***other information***. The first example above suggests that the Chairman's Report should be reworded, whilst the third suggests that the annual financial statements might require adjustment for the impairment.

* If the directors agree to the amendment, the auditor should adopt appropriate procedures to establish that the amendment rectifies the material inconsistency, e.g. ensuring that the re-wording of the chairman's report takes away the inconsistency.

* If the directors refuse to make amendments which are necessary in the ***annual financial statements***, the auditor will be forced to ***modify*** the audit opinion "***except for"*** or give an ***adverse*** opinion. For example, if impairment losses should be recognised in respect of inventory and the directors will not do so, an uncorrected misstatement will have arisen.

* If the directors refuse to make amendments which are necessary in the ***other information,*** the auditor will include an ***other matter*** paragraph in the audit report explaining the situation. Where the inconsistency is in the other information, a modification of the audit opinion paragraph is not appropriate as the financial statements ***do*** fairly present, it is the other information which is inconsistent.

5. *Examples of misstatements of fact*

* Employee information reflected in an employee highlights schedule has been incorrectly compiled (e.g. with the intention of deceiving employees).

* The report on Corporate Governance states that a social and ethics committee has been formed when in fact such a committee has not been formed.

* Certain persons of a particular gender or race have been listed as directors when they are not directors.

6. Action required by the auditor: misstatements of fact

The auditor should, by discussion with the directors and the audit committee (if applicable), attempt to have the material misstatement in the other information corrected. If the material misstatement was unintentional the directors are likely to make the necessary corrections to resolve the problem. However, all of the above examples suggest intentional misrepresentation so it may be appropriate for the auditor to suggest that legal advice be sought if the directors show reluctance to make the corrections. If the directors do refuse to correct the material misstatement of fact in the other information, the auditor should:

- notify the directors and the audit committee, in writing, of his concern
- consult with those charged with governance of the company
- take legal advice
- modify the auditor's report by including an ***other matter*** describing the misstatement of fact. Note: a modification of the audit opinion is not an option as the problem lies in the other information ***not*** the financial statements.
- consider whether there are any Section 45 Auditing Profession Act 2005 (reportable irregularity) responsibilities. This may be particularly important where the auditor considers that the directors are deliberately intending to deceive users in some way.

7. Note on the Directors' Report

The directors' report forms part of the annual financial statements prescribed by the Companies Act, and must be audited. However, the information in the directors' report is not in the form of an assertion and the subject matter is not identifiable and capable of consistent evaluation or measurement against identified criteria. Consequently the opinion expressed on the financial statements does not extend to the information contained in the directors' report as the auditor has no basis for concluding that the information is properly stated. In other words, the auditor cannot say that the directors' report "fairly presents" because there is no standard in which to judge the fair presentation of directors' reports.

Therefore for reporting purposes, the directors' report will be considered to be "Other information" as dealt with in ISA 720. The same will apply to the audit committee's report, and the company secretary's certificate.

CHAPTER 19

REVIEW ENGAGEMENTS AND RELATED SERVICE ENGAGEMENTS

CONTENTS

		Page
ENGAGEMENTS TO REVIEW HISTORICAL FINANCIAL STATEMENTS		19/2
1.	Introduction	19/2
2.	Companies which qualify for an independent review	19/2
3.	Description of a review engagement and comparison with an audit engagement`	19/2
4.	Objectives	19/5
5.	Ethical Requirements and professional scepticism	19/5
6.	Engagement level quality control	19/5
7.	Pre-conditions and preliminary engagement activities for a review engagement	19/6
8.	The engagement letter	19/6
9.	Performing the engagement	19/6
10.	Determining materiality	19/7
11.	Obtaining an understanding of the entity	19/8
12.	Inquiries and analytical procedures	19/9
13.	Performing additional procedures	19/10
14.	Procedures to address specific circumstances (including going concern)	19/11
15.	Reconciling the financial statements to underlying accounting records	19/12
16.	Written representations from management	19/12
17.	Forming the practitioner's conclusion on the financial statements	19/12
18.	Expressing a conclusion	19/13
19.	The Practitioner's Report	19/13
20.	Modifications	19/15
"AGREED UPON PROCEDURES" ENGAGEMENTS		19/17
1.	Introduction	19/17
2.	Objective	19/17
3.	General Principles	19/17
4.	Terms of Engagement	19/17
5.	Reporting Considerations	19/18
COMPILATION ENGAGEMENTS		19/19
1.	Introduction	19/19
2.	The Compilation Engagement	19/19
3.	Objectives	19/19
4.	Ethical Requirements	19/19
5.	Professional Judgement	19/20
6.	Engagement Level Quality Control	19/20
7.	Engagement Acceptance and Continuance	19/20
8.	Performing the Engagement (including compiling financial information)	19/21
9.	The Practitioner's Report	19/22

ENGAGEMENTS TO REVIEW HISTORICAL FINANCIAL STATEMENTS

1. Introduction

Whilst review engagements have been carried out by auditors for many years, the concept of an independent review of a company's financial statements replacing an external audit of a company's financial statements became an option with the promulgation of the Companies Act 2008. This option has resulted in a marked increase in the number of review engagements which practitioners are conducting and hence renewed interest in the relevant international standards on review engagements, particularly ISRE 2400 (Revised) – Engagements to review historical financial statements.

Sometimes it appears that a review engagement is just a very watered down audit and is not really important. Whilst a review does ***not*** give the same level of assurance as an audit, it is still an assurance engagement on which reliance is placed and which must be carried out in terms of the international standard.

2. Companies which qualify for an independent review

The option to be independently reviewed, as opposed to being externally audited, is determined by the public interest score of the company and whether the company's financial statements are internally or externally compiled.

2.1 A private company with a public interest score of less than 100 must (at least) have its financial statements independently reviewed regardless of whether its financial statements are internally or externally compiled. The review of this category's financial statements must be carried out by a Registered Auditor or an individual who qualifies to act as an accounting officer of a close corporation.

2.2 A private company with a public interest score of 100 to 349 may have its financial statements independently reviewed if its annual financial statements are externally compiled. (If the financial statements are internally compiled, the company must be audited). The review of the financial statements of companies in this category must be carried out by a Registered Auditor or a Chartered Accountant.

3. Description of a review engagement

3.1 The review of financial statements is a limited assurance engagement. ISRE 2400 (Revised) defines limited assurance as "the level of assurance obtained where engagement risk is reduced to a level that is acceptable in the circumstances of the engagement, but where that risk is greater than for a reasonable assurance engagement, as a basis for expressing a conclusion. The combination of the nature, timing and extent of evidence gathering procedures is at least sufficient for the practitioner to obtain a meaningful level of assurance. To be meaningful, the level of assurance obtained by the practitioner is likely to enhance the intended user's confidence about the financial statements".

The essence of this is that for a review, the practitioner will conduct sufficient procedures to give a level of assurance which will increase the level of confidence a user has that the financial statements are fairly presented, but not to the level of confidence which an audit would provide. An audit provides reasonable assurance, a review provides limited assurance.

3.2 In a review engagement, the practitioner performs primarily ***inquiry*** and ***analytical procedures.*** Obviously, he may choose to perform other types of procedure, e.g. observation, reperformance, etc, but the concentration in normal circumstances will be inquiry and analytical review to obtain sufficient appropriate evidence on which to base his conclusion.

Comparison of an audit engagement and a review engagement.

Factor	***Audit***	***Review***
1. Conducted by	Registered Auditor	PIS less than 100: Registered Auditor or individual who qualifies for appointment as an Accounting Officer. PIS 100 to 349: Registered Auditor or a CA(SA).
2. Assurance given	Reasonable Assurance	Limited assurance.
3. Standards	ISAs	ISRE 2400 (revised)
4. AFS compiled by	Client company	PIS less than 100: client or external party PIS 100 to 349: Independent accounting professional. (If internally compiled, AFS must be audited.)
5. Ethical considerations including objectivity to be applied	Yes	Yes
6. Professional scepticism to be adopted	Yes	Yes
7. Quality control procedures required	Yes	Yes
8. Pre-conditions and pre-engagement activities including an engagement letter.	Yes	Yes
9. Strategy	Audit strategy formulated	Not specifically required
10. Materiality	Planning, performance and final (evaluation)	Materiality set for the financial statements as a whole to • Identify areas of the financial statements where ***material*** misstatements may arise • Evaluate whether financial statements are free from material misstatement.
11. Understanding of entity	Yes, to identify and evaluate risks of material misstatement.	Yes, to identify where material misstatement may arise and provide a basis for designing procedures to address these areas.
12. Understanding internal control.	Detailed understanding.	General understanding.

13. Risk assessment procedures.	Yes, as a basis for determining further audit procedures (nature, timing and extent).	No
14. Tests of controls.	Yes	No
15. Substantive tests.	Full range	Usually inquiry and analytical procedures but may use other substantive procedures including tests of detail if ***additional*** procedures are required.
16. Going concern procedures.	Yes	Yes
17. Related party procedures.	Yes	Yes
18. Fraud procedures.	Yes	Yes
19. Report 19.1 title 19.2 addressee (usual) 19.3 responsibility paragraphs 19.4 Description of engagement 19.5 Explanation of modification paragraph 19.6 Opinion/conclusion wording 19.7 Other reports required by Companies Act paragraph. 19.8 Modification of opinion/conclusion. 19.9 Emphasis of Matter.	Opinion Independent Auditor's Report Shareholders Directors and Auditors Yes describe audit Yes In our opinion ……..fair presentation has been achieved in all respects. Yes Opinion: except for Adverse Disclaimer Yes	Conclusion Independent Reviewer's Report Shareholders Directors and Reviewers Yes describe review and emphasise that it is ***not*** an audit. Yes Based on our review nothing has come to our attention that causes us to believe that fair presentation has not been achieved in all material respects. Yes Conclusion: except for adverse disclaimer Unlikely. Not provided for in ISRE 2400.
20. Reportable Irregularity duties.	Yes, in terms of Auditing Professional Act 2005. Report to IRBA	Yes, in terms of Companies Regulations 2011 Report to CIPC.

4. Objectives

The objectives of the practitioner conducting a review engagement are to

4.1 Obtain ***limited*** assurance about whether the financial statements as a whole, are free of material misstatement, thereby allowing the practitioner to express a ***conclusion*** on whether anything has come to his attention that causes him to believe the financial statements are not prepared, in all material respects, in accordance with an applicable financial reporting framework, e.g. IFRS for SMEs. The limited assurance is obtained primarily by inquiry and analytical procedures.

4.2 Report on the financial statements. The report may contain a qualified or adverse conclusion and may even disclaim a conclusion.

5. Ethical Requirements and Professional Scepticism

5.1 As a review is an assurance engagement, the independence of the practitioner is an important ethical consideration. Thus the practitioner must be independent in mind and appearance. Likewise, the other fundamental principles of ethical/professional behaviour cannot be compromised because the engagement is a review and not an audit. The fundamental principles are

- integrity
- objectivity
- professional competence and due care
- confidentiality, and
- professional behaviour.

5.2 The adoption of an appropriate level of professional scepticism is important on a review engagement. Remember that professional scepticism is an attitude. It means that the practitioner does not just accept what he is told, or what he reads at face value. It also means that he does not allow himself to be "led around by the nose". It does not mean that in being sceptical, the practitioner abandons good professional behaviour. In the context of this type of engagement, professional scepticism means that the practitioner

- should question inconsistencies and investigate contradictory evidence
- should question the reliability of responses to inquiries and other information obtained from management and those charged with governance
- be alert to
  - evidence which is inconsistent with other evidence
  - information that calls into question the reliability of documents and responses to inquiries
  - conditions which may indicate fraud
  - any other circumstances which suggest the need for additional procedures, e.g. missing documents, lack of knowledge displayed by employees relating to inquiries.

Adopting an appropriate level of professional scepticism will reduce the risk of the practitioner overlooking unusual circumstances, over-generalising when drawing conclusions from evidence and of using inappropriate assumptions in determining the review plan and in the evaluation of evidence gathered. In a sense, professional scepticism guards against the review team treating a review engagement as "not that important" as referred to in the introduction to this chapter.

6. Engagement level quality control

The review engagement partner must possess competence in assurance skills and techniques (e.g. professional judgement, evaluating evidence, understanding information systems) and must take responsibility for

- the engagement being performed in accordance with the firm's quality control policies including being satisfied with
  - the pre-engagement procedures including the integrity of management
  - the collective competence and capabilities of the engagement team.
- the direction, supervision, planning and performance of the review
- the appropriateness of the review report/conclusion.

7. Pre-conditions and preliminary engagement activities for accepting a review engagement

7.1 Before accepting any assurance engagement (audit or review), the practitioner will carry out preliminary engagement activities, i.e.

* determining whether the practitioner wishes to establish or continue a ***professional relationship*** with the prospective/existing client
* considering the ***integrity*** of the client's principle owners, key management and those charged with governance
* determining whether the firm is ***competent*** to perform the engagement; skills, knowledge and resources
* determining whether the firm complies with ***ethical*** requirements, e.g. independence.

7.2 In addition and perhaps even prior to considering the above, the practitioner must satisfy himself that the pre-conditions for accepting a review engagement are present, i.e. he must

* determine whether the financial reporting framework applied in the preparation of the financial statements to be reviewed, is acceptable, e.g. IFRS or IFRS for SMEs
* obtain the agreement of management that it acknowledges and understands its responsibilities
  - for the preparation of the financial statements in accordance with the applicable financial reporting framework
  - for such internal control as management determines is necessary to enable the preparation of the financial statements that are free from material misstatement, whether due to fraud or error
  - to provide the practitioner with access to all information of which management is aware is relevant to the preparation of the financial statements, e.g. records, documentation, etc
  - to provide the practitioner with any additional information which he may request for the review
  - to provide, as well as any unrestricted access to persons within the entity, in the case where the financial statements have been compiled by an independent accounting professional, access to that individual.

The importance of the above points is confirmed by the fact that if the practitioner is not satisfied with any of the above pre-conditions, he should attempt to have the matter resolved by management and those charged with governance. Should the auditor still not be satisfied, the practitioner should ***not*** accept the engagement.

8. The engagement letter

Much of what is covered in the pre-conditions for accepting a review engagement will be recorded in an engagement letter. ISRE 2400 (Revised) requires that an engagement letter be obtained which deals with the following

* the intended use and distribution of the financial statements (and any restrictions thereon)
* identification of the applicable financial reporting framework
* the objective and scope of the review
* the responsibilities of the practitioner
* the responsibilities of management
* a statement that the engagement is ***not*** an audit and that the practitioner will not express an audit opinion on the financial statements
* reference to the expected form and content of the report and a statement that the form and content may differ from its expected form and content
* arrangements concerning the involvement of other practitioners and experts in the review. For example, the independent accounting professional who compiled the financial statements (applicable to reviews for companies with a public interest score between 100 and 349 which have their financial statements externally compiled)
* the expectation that management will provide written representations
* a request for management to acknowledge receipt of the engagement letter and to agree to the terms of the engagement.

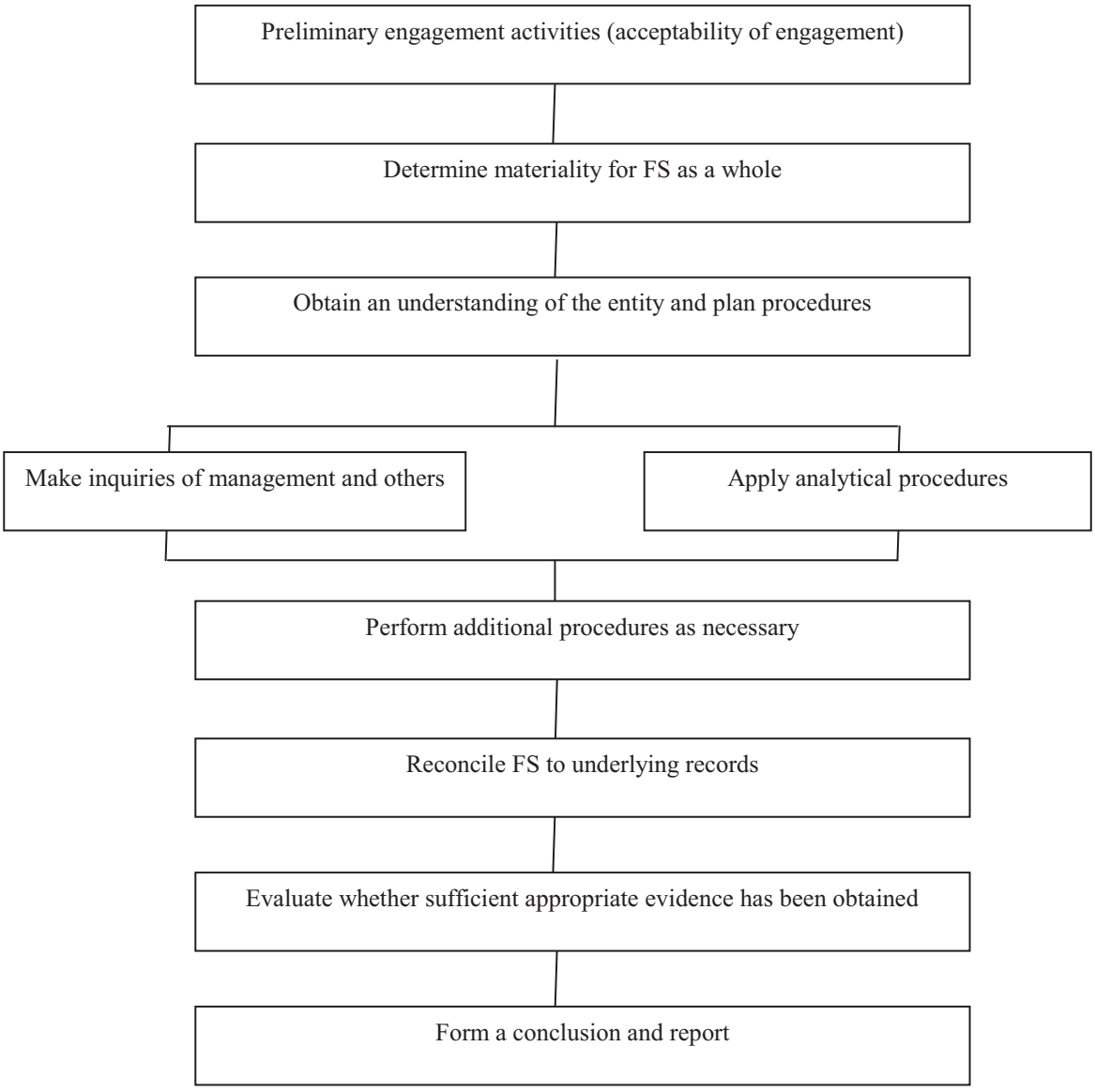
9. Performing the engagement

9.1 When considering an audit engagement, the process is reasonably well defined and extensively dealt with in the ISAs which cover specific aspects of the process, e.g. planning, identifying risks, materiality, audit evidence, etc. The independent review does not have a similar set of its own

statements and is guided by the content of ISRE 2400 (Revised). However, this does not mean that the content and principles contained in the ISAs are not relevant to varying degrees, e.g. the principles of audit evidence apply equally to reviews and in fact, the reviewing practitioner's "toolbox" is the same as that of the auditor. The difference is the emphasis which is placed on the use of available procedures. In a review, the emphasis will be placed on the use of inquiry and analytical procedures, but this does not preclude the reviewer from observation, external confirmation, recalculation and reperformance.

9.2 Furthermore, whilst it is not as detailed and defined as the audit process, there is a review process which must be adhered to if compliance with ISRE 2400 (Revised) is to be achieved. Diagrammatically it can be represented as follows

9.3 Diagrammatical representation of the review process



10. Determining materiality

10.1 ISRE 2400 (Revised) requires that the practitioner shall determine materiality for the financial statements as a whole and apply this materiality in designing procedures and evaluating results. For a review engagement, the practitioner is required to identify areas in the financial statements where ***material*** misstatements are likely to arise and to provide limited assurance on whether the

financial statements are free from ***material*** misstatement. The practitioner sets materiality for the engagement so that he has a guideline to work with.

10.2 There is no magic formula for determining materiality. The practitioner must apply professional judgement. The concept of materiality in any assurance engagement proposes that misstatement will be material if it could reasonably be expected to influence the economic decisions of users. Thus the practitioner will attempt to evaluate what "amount" of misstatement the users of the reviewed financial statements would tolerate. This is no easy task!

10.3 Note, that in a review engagement, because it consists primarily of inquiry and review, the practitioner does not set performance materiality (as for an audit), as performance materiality is used for determining the extent of testing for particular classes of transactions, account balances, or disclosures.

10.4 As with audit materiality, review engagement materiality is both quantitative and qualitative, which means that a misstatement which may be quantitatively immaterial, may have a qualitative aspect to it, e.g. it may be related to fraud, or it may relate to inadequate or omitted disclosures which are qualitatively material.

10.5 For the purposes of determining materiality for a review engagement, the practitioner must be mindful of the "types" of users of the financial statements he is reviewing and their needs. The majority of review engagements will be carried out on companies with low public interest scores and will tend to be smaller companies. The users of financial statements of companies with a public interest score of less than 100, would probably be restricted to the shareholders (usually a limited number), the bank and perhaps other finance providers. In these circumstances, it is acceptable for the practitioner to assume that users will simply be seeking some "comfort" (limited assurance) that the financial statements reflect a reasonably fair representation of the state of the company. For example, a shareholder who is not involved directly in the company, might use the financial statements to broadly assess how the company is doing and the bank may be seeking some assurance that the overdraft it is providing, is reasonably secure and that the value of inventory which has been offered as security for the overdraft, is not materially misstated. Perhaps the point to be made is that if a user is making important decisions of some magnitude or serious consequence, an audit opinion and not a review conclusion would be required.

11. Obtaining an understanding of the entity

11.1 The practitioner is required to obtain an understanding of the entity to provide the background against which he plans and performs the engagement and exercises his professional judgement. The major purpose of this is to identify where material misstatements are likely to arise and thereby to provide a basis for designing procedures to address these areas.

11.2 Note, that on an audit engagement, the "understanding of the entity" phase is carried out to identify and evaluate the risk of material misstatement at financial level and at assertion level so that further audit procedures can be planned. This is not the case for a review engagement. Although not as detailed (as for an audit), the process of obtaining an understanding of the entity in a review engagement, enables the practitioner to

* plan and perform the engagement appropriately
* identify areas where misstatements are likely to occur
* prepare appropriate responses to such areas identified (i.e. appropriate inquiries and analytical procedures)
* identify information pertaining to the possibility of fraud, existence of related parties, unusual transactions, going concern issues, and non-compliance with laws and regulations
* evaluate responses to inquiries and results of analytical procedures
* assess the appropriateness of the selection and application of accounting policies and the adequacy of presentation and disclosure.

11.3 In terms of ISRE 2400 (Revised), the practitioner shall obtain an understanding of

* relevant industry, regulatory, legal and other external factors including the applicable financial reporting framework

- the nature of the entity, including
  - its operations
  - ownership and governance structures
  - types of investment the entity is making
  - the way the entity is structured and financed
  - the entity's objectives and strategies
- the entity's accounting systems and accounting records
- the entity's selection and application of accounting policies.

11.4 The statement makes the point that obtaining an understanding of the entity is a "continual dynamic process" of gathering, updating and analysing information ***throughout the engagement.*** Practitioners need to avoid simply carrying out a routine set of standard procedures without much thought and assuming that not much has changed since the previous engagement.

11.5 The statement also makes the point that the practitioner should gain an understanding of the "tone at the top" and the control environment, as these factors are likely to reveal much about management's attitude to fair financial reporting.

12. Inquiries and analytical procedures

12.1 To obtain sufficient appropriate evidence as a basis for his conclusion on the financial statements, the practitioner must design and perform inquiry and analytical procedures
- to address all material items in the financial statements, including disclosures
- to focus on addressing areas in the financial statements where material misstatements are likely to arise.

12.2 Remember that when conducting these procedures, the practitioner remains alert to
- evidence which is inconsistent with other evidence
- information that calls into question the reliability of documents and responses to inquiries
- conditions which may indicate fraud.

12.3 The practitioner's ***inquiries*** of management should include the following
- how management makes significant accounting estimates
- the identification of related parties and related party transactions and the purpose of those transactions
- whether there are significant, unusual or complex transactions, including
  - significant changes in the client's business activities
  - significant changes to the terms of contracts which may affect the client's financial statements, e.g. new debt covenants
  - significant journal entries or other adjustments to the financial statements
  - significant transactions occurring near the end of the reporting period
  - the existence of any actual, suspected or alleged fraud or non-compliance with regulations which could affect the determination of material amounts and disclosures in the financial statements, e.g. taxation regulations not adhered to
  - whether management has identified and addressed events occurring between reporting date and the date of the practitioner's report which require adjustment to, or disclosure in, the financial statements
  - the basis of management's assessment of the company's going concern ability
  - material commitments, contractual obligations or contingencies that have affected, or may affect, the financial statements.

12.4 Analytical procedures involve the evaluation of financial information through analysis of relationships among both financial and non-financial data. The practitioner's analytical procedures can address a number of objectives, e.g.
- when obtaining an understanding of the entity, the practitioner may perform a simple comparison of current and prior period's gross profit percentages to get an overall understanding of the "normality" of the current year gross profit. If there are material

changes, either positive or negative, the practitioner will investigate more closely, those factors affecting gross profit

- in identifying inconsistencies and variances from expected trends, values or norms, e.g. comparing the "days outstanding" ratio for debtors for the current and previous three years
- providing corroborative evidence in relation to other inquiry or analytical procedures, e.g. a marked reduction in the days outstanding debtors ratio, may corroborate the client's accountants representation that credit management controls have been significantly improved
- serving as an additional procedure when the practitioner becomes aware of a matter which he believes may cause the financial statements to be misstated, e.g. the practitioner conducts an in depth comparative analysis of inventory quantities by description, value, location, etc to provide additional evidence to support a large increase in the value of inventory reflected in the financial statements.

12.5 Analytical procedures can vary from simple to very complex statistical analysis

- simple comparison, e.g. monthly sales for current year to monthly sales for the prior three years by corresponding month
- ratio and trend analysis, e.g. comparison of current ratio period to period
- comparison of financial and non-financial data, e.g. payroll costs to number of employees
- statistical analysis, e.g. regression analysis.

12.6 In order to carry out the analysis, the practitioner will make use of information from most, if not all, of the following sources

- financial information for comparable prior periods, e.g. previous year, three years, etc
- information about ***expected*** operating and financial results, e.g. budgets and forecasts
- relationships among elements of financial information within the period, e.g. sales commissions (expense) to sales (revenue)
- information regarding the industry in which the client operates, e.g. industry norms for gross profit, industry averages for payroll expenses
- relevant non-financial information for current and prior periods, e.g. delivery costs to delivery vehicles, sales to sales personnel.

13. Performing additional procedures

13.1 Essentially the practitioner is required to conduct additional procedures if he becomes aware of a matter which causes the practitioner to believe that the financial statements may be materially misstated. The practitioner may be alerted to the matter in a number of ways, for example, he may consider that management are being evasive in responding to inquiries or that explanations for variances resulting from analytical procedures are inadequate. The practitioner may also be alerted by the non-availability of supporting documentation where it is required.

13.2 The practitioner can conduct whichever additional procedures he deems necessary to settle his concern that the financial statements may be materially misstated. The types of procedure the practitioner is most likely to conduct are

- additional inquiry which is more focused and probing
- additional analytical procedures but in greater detail and directed specifically at the affected amounts or disclosures
- substantive tests of detail
  - inspection of physical assets and documentation
  - reperformance/recalculation
- external confirmation.

Example 1. The practitioner's ratio analysis of accounts receivable suggests that the allowance for doubtful debts is materially understated. An important aspect of the allowance is the aging of debtors to identify long outstanding debts. Inquiries of management have not satisfied the practitioner. As an ***additional procedure*** the practitioner may decide to reperform the aging of a sample of debtors' balances.

Example 2. The practitioner believes that sales may be materially misstated. A comparison of sales by month revealed that sales for the last month of the year, are considerably higher than budget or the corresponding month for the previous year. Management's explanation is that "it was just a good trading

month" is unconvincing based on other broad analytical evidence. As an ***additional procedure*** the practitioner may decide to perform detailed "cut-off" tests to determine whether sales made ***after*** year end, have been incorrectly included in the sales for the last month prior to year end.

Example 3. The practitioner believes that plant and machinery may be materially overstated by the incorrect inclusion of leased items. Inquiry of the client's financial accountant gave the practitioner the impression that the financial accountant did not understand the financial reporting standards for leases. As an ***additional procedure*** the practitioner may decide to carefully read all lease contracts into which the client has entered, to determine whether any operating leases have been inappropriately capitalised as finance leases.

Example 4. The practitioner believes that the financial statements may be materially misstated by the omission of a significant contingent liability pertaining to a matter he identified in the minutes of directors meetings. Management and the directors consider that although a claim against the company has been lodged, nothing will come of it and the matter can be ignored. As an ***additional procedure*** the practitioner may request that management obtain an attorney's representation letter from the company's attorneys pertaining to litigation and claims.

14. Procedures to address specific circumstances

In addition to the general discussion on performing a review, ISRE 2400 (Revised) raised three specific matters in respect of which the practitioner must conduct procedures. These are

14.1 Related parties

In addition to making inquires at the "understanding the client" stage as to the existence and identity of related parties and related party transactions, the practitioner must remain alert for arrangements or information that may indicate related parties/related party transaction that have not been identified or disclosed to the practitioner. If the practitioner identifies significant transactions outside the client's normal course of business, the practitioner should inquire of management about

* the nature of the transactions
* whether related parties could be involved
* the business rationale (logic) behind those transactions, i.e. is it arms-length, or possibly designed to conceal misappropriation or manipulation of the financial statements?

14.2 Fraud and non-compliance with regulations

If there is an indication that fraud or non-compliance has taken place, the practitioner must

* communicate the matter to senior management and those charged with governance
* request management's assessment of the effects on the financial statements
* consider the effect if any, on the practitioner's report and determine whether there is a responsibility to report the occurrence or suspicion of fraud or illegal acts to anyone outside the entity. This requirement is very important in the South African context. The reason is that the Companies Regulations 2011, Regulation 29, places an obligation on the independent reviewer to report any "reportable irregularity" to the Commission (CIPC) if the practitioner (reviewer) is satisfied or has reason to believe that a reportable irregularity is taking place. The situation is very similar in nature and procedure to an auditor reporting a reportable irregularity to the IRBA in terms of the Auditing Profession Act 2005. Refer to Chapter 3 for a discussion on reportable irregularities.

14.3 Going concern

A review of a client's financial statements includes a consideration of the entity's ability to continue as a going concern. In many instances "going concern" will not be an issue but if the practitioner becomes aware of events or conditions that may cast significant doubt about the entity's ability to continue as a going concern, a proper assessment of "going concern" should be performed. The assessment of "going concern" on an audit and on a review will be similar. For a detailed discussion, refer to Chapter 15 of this text.

15. Reconciling the financial statements to the underlying accounting records

The practitioner must obtain evidence that the financial statements agree with the underlying accounting records. This simply requires that the practitioner trace the financial statement amounts and balances to the relevant accounting records such as the ledger, summary records or schedules such as the trial balance.

16. Written representations from management

16.1 Management is requested to provide ***written*** representations because they are far more reliable than oral representations and because they focus management's mind on what they are telling the reviewer. Oral communication with the practitioner may be simpler and less time consuming but also means that subsequently facts can be refuted and claims of "misunderstanding of what was said" can be made. If the communication is written, management are likely to be more truthful and careful in what they communicate to the practitioner. There are also some matters which the practitioner may not identify other than through a management representation. The written representation request should be carefully worded as it is an important source of evidence in a review engagement.

16.2 The document should include representations that

* management has fulfilled its responsibilities for the preparation of the financial statements in accordance with the applicable financial reporting framework (Note that even where an "independent accounting professional" has compiled the financial statements, management is still responsible) and has provided the practitioner with all relevant information and access to information
* all transactions have been recorded and reflected in the financial statements
* management has disclosed to the practitioner
  - the identity of the client's related parties, related party relationships and transactions of which management is aware
  - significant facts relating to frauds or suspected frauds
  - known, actual or possible non-compliance with laws and regulations
  - all information relevant to the going concern ability of the entity
  - where required, that all subsequent events have been adjusted for or disclosed in the financial statements
  - all material commitments, contractual obligations or contingencies
  - all material non-monetary transactions or transactions undertaken for no consideration.

16.3 If management does not provide "one or more" of the requested written representations, the practitioner should

* discuss with management and those charged with governance
* re-evaluate the integrity of management and evaluate the effect of this on the evidence gathered.

If the practitioner concludes that there is sufficient doubt about the integrity of management or management does not provide the representations requested, the practitioner must disclaim a conclusion.

17. Forming the practitioner's conclusion on the financial statements

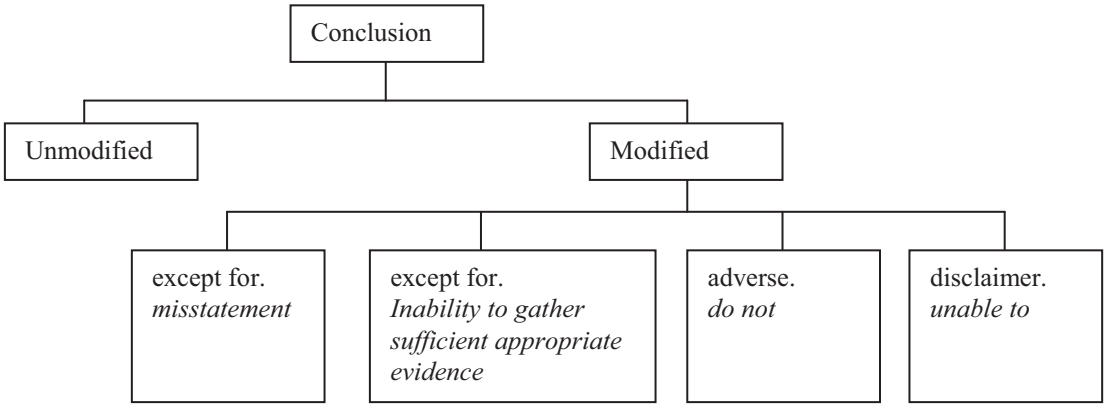
In forming the conclusion, the practitioner must

* evaluate whether the financial statements adequately refer to the financial reporting framework in terms of which they have been prepared, e.g. IFRS for SMEs
* consider whether (in the context of the reporting framework)
  - the terminology used in the financial statements is appropriate
  - the financial statements adequately disclose the significant accounting policies selected and applied
  - the accounting policies are consistent with the framework and appropriately applied
  - accounting estimates appear reasonable
  - the information presented in the financial statements appears relevant, reliable, comparable and understandable

- the financial statements provide adequate disclosures to enable users to understand the effects of material transactions and events on the entity's financial position, financial performance and cash flows
- the overall presentation, structure and content of the financial statements complies with the relevant framework
- whether the financial statements, including the notes, appear to represent the underlying transactions and events in a manner which achieves ***fair presentation.***

18. Expressing a conclusion

The practitioner has the following options with regard to the conclusion to be expressed on the financial statements



18.1 Unmodified conclusion

The practitioner gives an unmodified conclusion on the financial statements as a whole when he has obtained limited assurance to be able to conclude that nothing has come to his attention that causes him to believe that the financial statements do not fairly present, in all material respects, the financial position (at reporting date) of the entity, and its financial position and its cash flows for the year then ended, in accordance with the applicable financial reporting framework (e.g. IFRS for SMEs).

18.2 Modified conclusion – financial statements materially misstated (see para 20)

The practitioner shall give a modified conclusion on the financial statements as a whole when he determines that, based on the procedures performed and the evidence obtained, the financial statements are materially misstated. The practitioner will give

* a qualified conclusion "except for" where he concludes that the matter(s) giving rise to the modification, is material but ***not*** pervasive
* an adverse conclusion when the effects of the matter giving rise to the modification, are both material ***and*** pervasive.

18.3 Modified conclusion – inability to obtain sufficient appropriate evidence (see para 20)

The practitioner shall give a modified conclusion if he is unable to form a conclusion due to inability to obtain sufficient appropriate evidence. The practitioner will give

* a qualified conclusion "except for" where he concludes that the ***possible*** effects on the financial statements of undetected misstatements, if any, could be material but not pervasive
* disclaim a conclusion if he concludes that the possible effects on the financial statements of undetected misstatements if any, could be both material ***and*** pervasive.

19. The Practitioner's report

The practitioner's report on a review engagement has the same basic structure as the audit report but the wording is different due to the different nature of the engagement. The wording for the report in the South African context is contained in SAAPS 3 (Revised) which in turn, is based on ISRE 2400 (Revised).

19.1 Structure

* title
* the addressee

* introductory paragraph
* responsibility of directors' paragraph
* independent reviewer's responsibility paragraph
* a description of a review and its limitations paragraph
* an explanation paragraph when the conclusion is qualified or an adverse conclusion is given or a conclusion is disclaimed (e.g. basis for qualified conclusion)
* conclusion paragraph
* other reports required by the Companies Act paragraph
* signing off

19.2 Title – Independent reviewer's report

19.3 Addressee – To the shareholders of Keystone (Pty) Ltd

19.4 Introductory paragraph

We have ***reviewed*** the financial statements of Keystone (Pty) Ltd set out on pages 8 to 27, which comprise the statement of financial position as at 31 March 0001 and the statement of comprehensive income, statement of changes in equity and statement of cash flows for the year then ended, and the notes, comprising a summary of significant accounting policies and other explanatory information.

19.5 Directors' responsibility

The company's directors are responsible for the preparation and fair presentation of these financial statements in accordance with the International Financial Reporting Standard for Small and Medium-sized entities, and the requirements of the Companies Act of South Africa, and for such internal control as the directors determine is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

19.6 Independent reviewer's responsibility

Our responsibility is to express a ***conclusion*** on these financial statements. We conducted our review in accordance with the International Standard on Review Engagements ISRE 2400 (Revised) – *Engagements to Review Historical Financial Statements.* ISRE 2400 (Revised) requires us to conclude on whether anything has come to our attention that causes us to believe that the financial statements, taken as a whole, are not prepared in all material respects in accordance with the applicable accounting framework. This standard also requires us to comply with relevant ethical requirements.

19.7 Description of a review and its limitations (Note that this paragraph does not have a heading in the report. All other paragraphs do)

A review of financial statements in accordance with ISRE 2400 (Revised) is a limited assurance engagement. The independent reviewer performs procedures, primarily consisting of making inquiries of management and others within the entity, as appropriate, and applying analytical procedures, and evaluates the evidence obtained. The procedures performed in a review are substantially less than those performed in an audit conducted in accordance with International Standards on Auditing. Accordingly, we do not express an audit opinion on these financial statements.

19.8 Conclusion (unmodified)

Based on our review, nothing has come to our attention that causes us to believe that these financial statements do not fairly present, in all material respects, the financial position of Keystone (Pty) Ltd as at 31 March 0001 and its financial performance and cash flows for the year then ended in accordance with the IFRS for SMEs and the requirements of the Companies Act of South Africa.

19.9 Other Reports required by the Companies Act

As part of our independent review of the financial statements for the year ended 31 March 0001, we have read the Directors' Report for the purposes of identifying whether there are material inconsistencies between this report and the reviewed financial statements. The Directors' Report

is the responsibility of the directors. Based on reading the Directors' Report, we have not identified material inconsistencies between this report and the reviewed financial statements. However, we have not reviewed the Directors' Report and accordingly do not express a conclusion thereon.

19.10 Signing off (no heading)



Joseph January
Registered Auditor
15 May 0001
Patchwork Office Park
East London

20. Modifications

Where the reviewer's conclusion requires modification, a paragraph must be included in the report explaining the modification. This paragraph will be positioned above the conclusion paragraph and will be headed according to the type of modification. The options are

*	except for conclusion	:	Basis for qualified conclusion
*	adverse conclusion	:	Basis for adverse conclusion
*	disclaimer of conclusion	:	Basis for disclaimer of conclusion

There is no standard wording for "Basis for" paragraphs. The paragraph must be sufficiently clear and detailed to the extent the user needs to understand the modification.

20.1 Except for conclusion

An except for conclusion is given where the matter on which the modification to the conclusion is based, is material but not pervasive. The modification can be based on misstatement or inability to obtain sufficient appropriate evidence. When an except for conclusion is given, the wording of the other paragraphs does not change. The conclusion paragraph will be headed "Qualified Conclusion" and will be worded as follows

* Misstatement. "Based on our review, except for the effects of the matter described in the Basis for Qualified Conclusion paragraph, nothing has come to our attention....."
* Inability to obtain sufficient appropriate evidence. "Based on our review, except for the ***possible*** effects of the matter described in the Basis for Qualified Conclusion paragraph, nothing has come to our attention....."

20.2 Adverse conclusion

An adverse conclusion is given when the financial statements are materially misstated and the misstatement is deemed to be ***pervasive*** to the financial statements. When an adverse conclusion is given, the wording of the other paragraphs does not change. The conclusion paragraph will be headed "Adverse Conclusion" and will be worded as follows

* "Based on our review, due to the significance of the matter discussed in the Basis for Adverse Conclusion paragraph, we conclude that these financial statements ***do not*** present fairly, the financial position of....."

20.3 Disclaimer of conclusion

A disclaimer of conclusion is given when the reviewer was unable to obtain sufficient appropriate evidence about multiple elements of the financial statements. The effect of this inability is that the practitioner is unable to complete the review and thus unable to form a conclusion. This has ramifications for the wording in other paragraphs in the report which are explained below. The conclusion paragraph will be headed "Disclaimer of Conclusion" and will be worded as follows "Due to the significance of the matters described in the Basis for Disclaimer of Conclusion paragraph, we were unable to obtain sufficient appropriate evidence to form a conclusion on these financial statements. Accordingly, we do not express a conclusion on these financial statements".

Changes to other paragraphs when a disclaimer is given, will be as follows

- in the Introductory paragraph, the words “We have reviewed.....” will change to “We were engaged to review.....”
- the wording in the Independent Reviewer’s Responsibility paragraph is replaced by the following wording “Our responsibility is to express a conclusion on these financial statements. Because of the matter described in the Basis for Disclaimer of Conclusion paragraph, however, we were not able to obtain sufficient appropriate evidence as a basis for expressing a conclusion on the financial statements”.

"AGREED UPON PROCEDURES" ENGAGEMENTS

1. Introduction

ISRS 4400 - Engagements to perform agreed upon procedures regarding financial statements, provides guidance on this related services engagement (ISRS stands for International Standards on Related Services). Although the engagement is referred to as an agreed upon procedures engagement, the report arising from the engagement is referred to as a factual findings report.

2. Objective

In an "agreed upon procedures" engagement, the auditor is engaged to carry out procedures (usually of an audit nature) which have been agreed upon by the parties involved, e.g. the auditor, the client and any interested third party. The auditor reports only on the facts as found. ***No assurance is given***, neither in the form of an audit opinion nor in the form of a review conclusion. The users of the report are required to draw their own conclusions from the facts presented.

3. General principles of an agreed upon procedures engagement

3.1 General ethical principles to which practitioners are expected to adhere for this type of engagement, remain the same as for any engagement, e.g.

* integrity
* objectivity
* professional competence and due care
* confidentiality
* professional behaviour.

Note: independence from the client is not a requirement for this type of engagement. However, the practitioner is still required to be objective in the performance of the engagement. Where the practitioner is ***not*** independent, a statement to that effect must be made in the report arising from the engagement.

3.2 The practitioner must comply with ISRS 4400.

3.3 The engagement must be properly planned so that an effective engagement will be performed.

3.4 The practitioner must maintain appropriate documentation to

* support the report on factual findings and
* provide evidence that the engagement was carried out in terms of ISRS 4400.

3.5 The practitioner must carry out the procedures agreed upon and use the evidence obtained as a basis for the report of factual findings. Procedures to be agreed upon may include:

* inquiry and analysis
* recomputation, comparison and other clerical accuracy checks
* observation
* inspection
* obtaining confirmations.

4. Terms of engagement

4.1 As with any engagement it is important that the terms of engagement are clear to all parties e.g. the client must understand that in this type of engagement ***no*** assurance is given. The terms of engagement should be set out in an engagement letter and should include:

* a clear indication that the engagement does not constitute an audit or review and that accordingly no assurance will be given
* the purpose of the engagement
* identification of the financial information to which the agreed upon procedures will be applied
* nature, timing and extent of the specific procedures to be applied
* anticipated form of the report of factual findings
* limitations on the distribution of the report
* a listing of the procedures to be performed that were agreed upon.

5. Reporting considerations

5.1 Title: Report of Factual Findings.

5.2 Addressee: To the directors of Pentel Ltd (will be whoever engaged the practitioner).

5.3 Description of the engagement*

We have performed the procedures agreed with you and described below with respect to the accounts payable of Pentel Ltd... as at (date), set forth in the accompanying schedules. Our engagement was undertaken in accordance with the International Standard on Related Services applicable to agreed upon procedures.. The procedures were performed solely to assist you in evaluating the validity of the accounts payable and are summarised as follows:...

Note: A summary of the procedures would be inserted here ***followed*** by the results of the procedures conducted.

5.4 Explanation of the nature of the report*

Note: As indicated, ***no*** assurance is given. The report is simply a presentation of the findings arising from the performance of the agreed upon procedures. To emphasise this, the following paragraphs are included in the report.

* *Because the above procedures do not constitute either an audit or a review made in accordance with International Standards on Auditing or International Standards on Review Engagements, we do not express any assurance on the accounts payable as at* (date).
* *Had we performed additional procedures or had we performed an audit or review of the financial statements in accordance with International Standards on Auditing or International Standards on Review Engagements, other matters might have come to our attention that would have been reported to you.*

5.5 Modified factual findings reports

Note: As no assurance is given, qualification is ***not*** an option. No Emphasis of Matter paragraph can be added. The results are presented ***without*** opinion or conclusion.

5.6 Closing paragraph*

Note: The report is signed in the normal manner (see comments on page 18/5) but above the signing off, the following paragraph is added to clarify the restricted nature of the engagement and report

* *Our report is solely for the purpose set forth in the first* (description of engagement) *paragraph of this report and for your information and is not to be used for any other purpose or to be distributed to any other parties. This report relates only to the accounts and items specified above and does not extend to any financial statements of Pentel Ltd , taken as a whole.*

5.7 Signing off*

Roddy Rockett
Rodney Rockett
Registered Auditor
15 March 0001
116 Vista Park
Durban

* The factual findings report does not have paragraph headings. They have been included here to convey the structure and content of the report. The wording of the paragraphs is in italics.

COMPILATION ENGAGEMENTS

1. Introduction

Much like the review engagement, practitioners have been conducting compilation engagements for many years. However, the requirements of the Companies Act 2008 and the Companies Regulations 2011, have increased the importance and frequency of these engagements. In terms of Regulation 29, a company which is not required to be audited, must have its annual financial statements independently reviewed. A ***private*** company will qualify to have its annual financial statements reviewed if

* it has a public interest score of 100 to 349, and
* the company's annual financial statements are ***compiled externally*** by an "independent accounting professional" as defined in Regulation 27.

A registered auditor (or chartered accountant) will satisfy the definition of accounting professional and as long as such individual is independent of the client, e.g. no financial interest in the client, not involved in the day to day running of the client etc, he may undertake a compilation engagement as envisaged by the International Standards on Related Services ISRS 4410 (Revised). It is likely therefore that accounting and auditing firms will experience an increase in the frequency of compilation engagements. Of course, a registered auditor or chartered accountant who ***compiles*** the financial statements may not also perform the review (or audit) of those financial statements.

2. The compilation engagement

2.1 Definition

An engagement in which the practitioner applies accounting and financial reporting expertise to assist management in the preparation and presentation of financial information of an entity in accordance with an applicable financial reporting framework, and reports as required by ISRS 4410 (Revised).

2.2 The value to users of financial information compiled in accordance with ISRS 4410 (Revised) arises from the ethical application of the practitioner's professional expertise. It is very important therefore that the practitioner complies with the required professional standards, both "technical" and "ethical". A compilation engagement is not just a matter of picking up a trial balance from a client and drawing up a set of financial statements; the practitioner must comply with ISRS 4410 (Revised) to the extent that its requirements are satisfied.

2.3 Management retains responsibility for the financial information and the basis on which it is prepared. For example, it is not the responsibility of the compiling practitioner to select accounting policies or decide upon appropriate estimates/allowances.

2.4 A compilation agreement is ***not*** an assurance engagement. It does not require the practitioner to verify the accuracy or completeness of the information provided by management, or otherwise to gather evidence to express an audit opinion or review conclusion.

This text deals primarily with the application of ISRS 4410 (Revised) in the context of the compilation of annual financial statements in terms of IFRS for SMEs.

3. Objectives

The practitioner's objectives are to

3.1 Apply accounting and financial reporting expertise to assist management in the preparation and presentation of financial statements in accordance with IFRS for SMEs.

3.2 Report in accordance with the requirements of ISRS 4410 (Revised).

4. Ethical requirements

4.1 In terms of the Code of Professional Conduct, the fundamental principles are

* integrity
* objectivity
* professional competence and due care
* confidentiality
* professional behaviour.

4.2 The fundamental principle of ***integrity*** requires, inter alia, that the practitioner should ***not*** be associated with information which he believes to be false, misleading (by inclusion or exclusion) or recklessly provided. This is clearly applicable to any financial statements which a practitioner compiles and if the situation (false, misleading, reckless) arises, the practitioner must take steps to disassociate himself from the financial statements.

4.3 Whilst the fundamental principle of ***objectivity*** is applicable to a compilation engagement, the requirements of Sec 290 – Independence – Audit and Review Engagements, do not apply to compilation engagements.

5. Professional judgement

There are a number of matters in a compilation agreement which require the application of sound professional judgement. These include judgement on ethical and technical matters. Important matters requiring professional judgement include

* the acceptability of the financial reporting framework to be used. For example, does the entity satisfy the scoping requirements for the application of IFRS for SMEs?
* assisting management with the selection of appropriate accounting policies
* assisting management with accounting estimates, e.g. impairments
* preparation and presentation of the financial information in accordance with IFRS for SMEs.

6. Engagement level quality control

The engagement partner must take responsibility for the overall quality level of the compilation engagement to which he is assigned. This includes

* following appropriate procedures for the acceptance of a new compilation engagement client or continuing with an existing compilation engagement client
* being satisfied that the engagement team has the necessary competence and capabilities
* being alert to the possibility of non-compliance by members of the engagement team with ethical requirements, e.g. disclosing confidential client information, showing a lack of due care
* directing, supervising and performing the engagement in compliance with professional standards and applicable legal/regulatory requirements
* taking responsibility for the maintenance of appropriate engagement documentation.

7. Engagement acceptance and continuance

A compilation agreement should ***not be accepted*** unless the practitioner has agreed the terms of engagement with management in an ***engagement letter.*** This includes

7.1 The intended use and distribution of the financial information, e.g. the annual financial statements are compiled for the purposes of having the independent review conducted in terms of the requirements of the Companies Regulation Number 29. Initial distribution will be to Joseph Soap and Co, Registered Auditors, who will conduct the review. Thereafter distribution will be to the bank and the company's shareholders. Restrictions on distribution should also be stated.

7.2 Identification of the applicable financial reporting framework, e.g. IFRS for SMEs.

7.3 The objective and scope of the compilation engagement, see paragraph 3.

7.4 The responsibilities of the practitioner, including compliance with relevant ethical requirements, e.g. no association with false, misleading information.

7.5 The responsibilities of management for

* the financial information and for the preparation and presentation thereof in accordance with a reporting framework which is acceptable in relation to the intended use thereof
* the accuracy and completeness of the records, documents, explanations and other information provided by management
* judgements needed in the preparation and presentation ***including*** those judgements with which the practitioner may assist management
* the expected form of the practitioner's report.

7.6 Conveying that the engagement is not an assurance engagement.

7.7 Conveying that the practitioner will not express an audit opinion or a review conclusion.

7.8 Arrangements concerning the involvement of a predecessor practitioner if any, and other practitioners or experts if any.

7.9 The possibility that management or those charged with governance may be requested to confirm in writing, certain explanations/information conveyed orally to the practitioner.

7.10 Arrangements for the ownership of the practitioner's engagement documentation.

7.11 A request to management to acknowledge receipt of the engagement letter and to agree to the terms of engagement included in the letter.

8. Performing the engagement

8.1 The practitioner's understanding

The practitioner cannot compile a set of financial statements for a client in a vacuum. The practitioner should obtain an understanding of

* the client's business and operations, including the company's accounting system and accounting records
  - the nature of the entity's assets, liabilities, revenues and expenses
  - the size and complexity of the entity and its operations
  - the level of development of the entity's management and governance structures regarding their management and oversight of the entity's accounting records and financial reporting system
  - the complexity of the financial reporting system and the principles and practices of the industry in which the client operates.
* the applicable financial reporting framework e.g. a good knowledge of IFRS for SMEs.

Obtaining an understanding is an ongoing process throughout the engagement. The understanding establishes a frame of reference within which the practitioner can exercise professional judgement.

8.2 Compiling the financial information

* the practitioner will compile the financial statements using the records and documents supplied by management. Other information and explanations will also be necessary and should come from management as well. The practitioner should be given access to what he considers necessary to carry out the compilation
* if in the course of carrying out the compilation, the practitioner becomes aware that any of the documents, records, information or explanations (including any significant judgements) are ***incomplete, inaccurate*** or ***otherwise unsatisfactory***, he must
  - bring it to the attention of management, and
  - request the additional or corrected information
* if the practitioner is unable to complete the engagement because management has failed to provide the necessary records, documents, explanations or other information as requested by the practitioner, the practitioner must withdraw from the engagement and inform management and those charged with governance, as to the reasons for withdrawing
* if the practitioner believes that amendments to the compiled financial statements are needed to ensure that they are not materially misstated, the practitioner cannot simply make the amendment but must propose the appropriate amendment to management.

Example 1. The practitioner may become aware from reading the directors' minutes that a piece of machinery has been damaged. A discussion with management revealed no impairment of the machinery which was required and was material, had been recognised.

Example 2. The practitioner realises from the documentation he has been presented with, that a material contingent liability has been omitted from the notes to the financial statements.

* if these types of situation arise, the practitioner will need to make a decision on the ***materiality*** of the matter. Materiality in this situation will be judged in the normal manner,

i.e. the matter will be material if "the misstatement or omission could reasonably be expected to influence the economic decisions of users based on the financial statements"

* if management declines to make the required adjustments, the practitioner must withdraw from the engagement and inform management and those charged with governance of the reasons for withdrawing. Note that the practitioner does ***not*** have the option of "qualifying" the compilation report. The compilation can either be achieved or it can't. Also be mindful of the fact that the auditor cannot be associated with a set of financial statements which he knows to be false, misleading or recklessly provided. If the financial statements are materially misstated, they will be at least misleading, and the practitioner must withdraw.

9. The practitioner's report

The practitioner's report is reasonably short and uncomplicated. As mentioned earlier, there is no opportunity for giving an "except for" or adverse opinion, a disclaimer of opinion or an emphases of matter. No opinion is given nor is any conclusion drawn.

Note. Paragraph headings marked * are not included. The headings have been provided simply to describe the structure and content of the report.

9.1 Title : Practitioner's compilation report.

9.2 Address : To the management of Towrite (Pty) Ltd.

9.3 Introductory paragraph*

We have compiled the accompanying financial statements of Towrite (Pty) Ltd based on information you have provided. The financial statements comprise the statement of financial position of Towrite (Pty) Ltd at 28 February 0001, the statement of comprehensive income, statement of changes to equity and statement of cash flows for the year then ended, and a summary of significant accounting policies and other explanatory information.

9.4 Practitioner's "role"*

We performed this compilation engagement in accordance with the International Standard on Related Services 4410 (Revised) – Compilation engagements. We have applied our expertise in accounting and financial reporting to assist you in the preparation and presentation of these financial statements in accordance with International Financial Reporting Standards for Small and Medium-sized entities (IFRS for SMEs). We have complied with relevant ethical requirements, including principles of integrity, objectivity, professional competence and due care.

9.5 Management's responsibility*

These financial statements and the accuracy and completeness of the information used to compile them are your responsibility.

9.6 Reliance*

Since a compilation engagement is not an assurance engagement, we are not required to verify the accuracy or completeness of the information you provided to us to compile these financial statements. Accordingly, we do not express an audit opinion or a review conclusion on whether these financial statements are prepared in accordance with IFRS for SMEs.

9.7 Signing off*

Freddie Filander

Frederick Filander (may include professional designation)
15 April 0001
Fasttrack Park
Cape Town

Note. The above report is for a set of general purpose financial statements prepared in terms of IFRS for SMEs, primarily because this is the most common compilation engagement likely to be undertaken by auditing and accounting firms. A compilation engagement can be carried out in respect of other information including modified financial reporting frameworks; the principles will remain the same.

DETAILED INDEX CHAPTER BY CHAPTER

Chapter 1 – Introduction to Auditing
Absolute assurance, 8
accounting bodies, 11, 12
assertions, 17, 18
assurance engagements, 6, 8
. levels, limited, reasonable, other
attributes of a profession, 10
auditing profession act, 17
companies act and companies regulations, 12,13, 15, 16
elements of assurance engagement, 6, 8
financial reporting, 9
financial statement audit engagement, 13
IFRS 6, 7, 15
independence, 2, 3, 4
internal controls, 9, 22
IRBA, 4, 10, 11, 12
ISAs, 17
ISA 200 – overall objectives of the auditor, 8, 15
ISA 315 (revised) – identifying and assessing risks, 17
limitations of an audit, 8
limited assurance, 8
need for auditors, 5
non-assurance engagements, 7, 8
postulates of auditing, 20
professional judgement, 19
professional scepticism, 19
professional status, 21
pronouncements to regulate the profession, 12
public interest/scores, 13, 14
reasonable assurance, 8
review engagement, 7, 14
role of shareholders, directors & auditors, 16
SAICA, 10, 11, 12
theory of auditing, 2
types of auditor, 2, 3, 4, 15, 20
. external, internal, government, forensic,
. special purpose
what is an auditor, 2

Chapter 2 – Professional conduct
advertising, 8
audit & review engagements, 24
client acceptance, 17
client's assets, 23
chartered accountants, 2, 3, 13, 38, 46
. public practice 2, 13
. in business 3, 46
code of ethics, 3, 4
code of professional conduct, 2, 3, 5
conceptual approach, 5, 23
conceptual framework, 5, 24, 46
confidentiality, 7
conflicts of interest, 6, 19, 48
engagements, 17, 22
ethics, 3, 4
family & personal relationships, 30
fees, 21, 42
financial interests, 27, 50
fundamental principles, 5
gifts/hospitality, 22, 45
independence, 2, 24-45
inducements, 51
integrity and objectivity, 3, 6, 37
IRBA, 3, 44
loans, guarantees, 29
marketing , 22
objectivity 7, 24, 37
professional appointment, 17, 18
professional behaviour, 8, 37
professional competence, 7

Chapter 2 – Professional conduct (continued)
public interest, 4
publicity, 8
recruiting, 10
reports, 9
reporting, 49
responsibility to colleagues, 10
safeguards, 12-52
SAICA, 3-5
second opinions, 20
tax services, 36
threats, 10, 17, 46-52
. self-interest, 10, 14, 15, 27-46
. self-review, 11, 15, 33-42
. advocacy, 11, 15, 33-41
. familiarity, 11, 16, 28, 30, 31, 32, 33, 34, 41, 45
. intimidation, 11, 16, 29, 30, 31, 42, 45

Chapter 3 – Statutory
Companies Act 2008, 3
annual financial statements, 25
audit committees, 40, 53
auditors, 51
. appointment, 51
. resignation, 52
. rotation, 52
board committees/meetings, 40- 44
business rescue & remedies, 57-64
categories of companies
. profit, 15, 23, 27, 40
. non-profit, 15
. private, 15, 50
. personal liability, 15
. public, 16, 50
company names, 17
company records, 23, 24
. access, 24
. accounting records, 23, 24
. financial year-end, 24
company secretary, 49-51
companies tribunal, 64
compliance with the Act, 5
directors, 40
. election, 41
. ineligibility and disqualification, 41
. removal, 42
. meetings, 43
directors' conduct, 45, 62, 63, 64
directors' liability, 46, 47
directors' personal financial interests, 44
distributions, 32
financial statements, 25
financial reporting standards, 7, 65
fundamental transactions, 55
. disposal of assets, 55
. amalgamations/mergers, 55
. scheme of arrangement, 56
governance, 35
incorporation of companies, 18
independent reviews, 9
intellectual property, 64
juristic person, 12, 50
legal status of companies, 20
loans to directors, 31
merging of companies, 55
memorandum of incorporation, 19, 20
names of companies, 17, 27
offences and penalties, 66
policy objectives for Companies Act, 3, 13, 14
practitioners functions, 59

Chapter 3 – Statutory (continued)
pre-incorporation contracts, 22
proxies, 35
public interest/scores, 6-8, 58
purpose of the Companies Act, 6, 8, 14
reckless trading, 22
record date, 36
registration of company, 17, 18, 23, 27
related and inter-related persons, 12
remedies and enforcement, 62
reportable irregularities, 8-10
rules, 19
securities, 34
shares, 27, 29
. authorisation, 27, 28
. capitalisation, 33
. distribution, 32
rights, 35, 36
. preference, rights, limitations, 28
. subscription and issue, 29
. consideration (price), 29
. issue to directors/related persons, 29
. securities, 30
. subsidiaries, 33
shareholders meetings, 33, 35, 36
. notice, 37
. conduct, 38
. quorum, 38
. resolutions, 39
social and ethics committee, 10, 40
solvency and liquidity test, 13
structure of the Act, 4
subsidiary relationships, 13
transparency, 23
whistle blowers, 63
winding up of companies, 48

Chapter 3 – Statutory
Close Corporation Act, 67
accounting and disclosure, 77
accounting officer, 78
administration of the act, 69
annual financial statements, 68, 77
association agreements, 74
audit requirements, 68
disqualification from managing business, 74
external relations, 76
fiduciary position to members, 73
founding statement, 69
internal relations, 73, 74
juristic person, 69
liability of members, 79
loans to members and others, 76
meetings, 75
membership, 71-73
MOI, 19, 20, 69, 82
payments to members, 75
public interest, public interest score, 8, 67, 77
pre-incorporation contracts, 76
unfairly prejudicial conduct, 75
variable rules regarding internal relations, 74

Chapter 3 - Statutory
Auditing Profession Act 2005, 80
accountability of registered auditors, 91
accreditation and registration, 81
conduct and liability of auditors, 83
general matters, 92
interpretation and objects of act, 80
IRBA, 80, 89
offences, 91
practice/duties, 83-89
registration, 81, 82
reportable irregularities, 85-93
structure of the act, 80

Chapter 4 – Corporate Governance, 3
alternate dispute resolution (ADR), 6, 36, 37
application of King III, 7
audit committees, 15, 17-21, 31
. existence, 17
. membership, 17
. responsibilities, 18
. internal assurance providers, 19
. external assurance providers, 21
background, 3
. King 1994, 3
. King, 2002, 3
boards and directors, 7-17, 29, 30, 32, 36, 38
. role and function, 9
. composition of board, 12
. appointment process, 13
. director development, 13, 14
. company secretary, 14
. performance assessment, 14
. board committees, 15
. group boards, 15
. remuneration, 16
. reporting, 21
. IT responsibility, 26
compliance with laws and regulations, 29
ethical leadership and corporate citizenship, 7
governing stakeholder relationships, 32-36
. stakeholders, 32
. dispute resolution, 6, 36, 37
integrated (sustainability) reporting, 19, 37
. transparency and accountability, 37
internal audit, 30-32
. need and role, 30
. approach, 30
. status, 31
IT governance, 6, 26-29
King III code of governance principles, 4
. basis, 4
. comply or explain, 4
. comply or else, 4
. apply or explain, 4
King III, 5
. leadership, 5
. sustainability, 5, 6
. corporate citizenship, 5
. innovation, fairness and collaboration, 6
. social transformation, 6
risk based – internal audit, 30
risk governance, 21
. responsibility, 23
. assessment, 23
. committee, 28
. management, 23, 29, 31
. response, 25
. assurance, 26
. monitoring, 25
. disclosure, 26
stakeholders, 32-36

Chapter 5 – General Principles of Auditing
access/custody controls 15
applicable controls, 17
appropriate evidence, 20
assertions, 23, 24
auditor's toolbox, 25
audit sampling, 29
comparison and reconciliation, 16
components of internal control, 5-20
control activities, 6, 12-18
control environment, 6, 7
definitions, 5, 29
external auditor's interest in internal control, 19
financial reporting, 9
financial statement assertions, 23

Chapter 5 – General Principles of Auditing (continued)
information system, 6
internal control and risk, 3
internal control, smaller entities, 18
isolation of responsibility, 15
ISA 315 (revised) Internal control, 5-8, 19, 27
ISA 500 audit evidence, 25
ISA 530 audit sampling, 29
monitoring controls, 6, 17, 19
preventive, detective, corrective controls, 12, 16, 17
reliability and relevance of evidence, 21, 22
risk assessment,6, 8-10
sampling, 29-33
segregation of duties, 13-15
statistical/non-statistical approach, 30
substantive procedures, 26, 28, 30
sufficient appropriate evidence, 20
tests of controls, 26, 27, 30
vouching and verifying, 28

Chapter 6 – Overview of the audit process
audit plan and strategy, 13-15
audit process, 6-8
diagram of audit process, 6
ethical requirements, 2
evaluating, concluding and reporting, 21
existing clients, 9
financial reporting standards, 23
further audit procedures, 20
ISAs, 2, 3, 4, 5, 8, 13, 16, 20, 21
materiality, 15
misstatements, 22
planning, 6, 7, 8, 13-18
preliminary engagement activities, 3, 4, 9-13
prospective clients, 9
quality control for audit of financial statements, 2
responding to assessed risk, 20-21
risk assessment, 8, 20-21
sufficient appropriate evidence, 22

Chapter 7 – Important elements of the audit process
Auditor's duties, 43
auditor's objective, 32
audit of financial statements – laws and regulations, 43
audit risk – components, 4, 6
. inherent limitations, 4, 6
. audit process, 4
. control risk, 5
. detection risk, 6
. relationship of different risks, 6
communication with management, 40, 41
components of audit risk, 5
entity and its environment, 9
. external factors, 11
. nature of entity, 11
. accounting policies, 13
. business risk, 13
. financial performance, 13
entity's internal control, 10, 14
. environment, 10, 11, 14
. risk assessment process, 15
. information system, 15
. control activities, 19
. monitoring controls, 19
fraud in audit of financial statements, 32
fraud – definition, 32
. auditor's responsibility, 34
. error, 32
. fraud risk factors, 32, 38, 40
. management fraud, 32, 37, 39, 41
. employee fraud, 32
. fraudulent financial reporting, 32, 37, 38
. management responsibility, 34

Chapter 7 – Important elements of the audit process (continued)
. misappropriation of assets, 33, 40
. retention of clients, 42
ISA 240, 32, 34
ISA 250, 43
ISA 315 (revised), 7, 10, 34, 43
ISA 320, 21
ISA 450, 21, 27
materiality, 21
. evaluating stage (final), 27, 31
. nature, 22
. planning and performance, 24-27
. qualitative/quantitative, 23, 26
. misstatements, 27, 28, 29, 35
reporting of non-compliance, 44
responses to fraud, 35
. at assertion level, 35
. at financial statement level, 35, 43
. evaluation of evidence, 37
. management override & representations, 36, 37, 41
risk assessment procedures, 8, 34
. analytical procedures, 9
. client acceptance, 8
. discussion with audit team, 10
inherent risk, 5
. inspection, 9
. inquiries of management, 8
. observation, 9
significant risks, 20, 21
understanding audit risk, 4
understanding the entity & environment, 7, 10, 11

Chapter 8 – Computer audit – basics
access controls, 16, 30
application controls, 26-41
. segregation of duties, 27
. isolation of responsibilities, 28
. approval & authorisation, 28
control activities, 27
. custody, 29
. access controls, 30
. comparison & reconciliation, 31
. performance reviews, 32
. batching, 32-34
. screen aids, 34-35
. processing controls and input, 35
. output controls, 38
. logs and reports, 39
. masterfile amendments, 39-40
programme checks, 35-38
CAATs (computer assisted audit techniques) 41
. audit process, 41
auditing around, through and with the computer, 42, 43
. system orientated caats, 43
. data orientated caats, 45
. decision to use caats, 45
. audit functions, 46-47
control environment, 5, 8
diagram for IT department, 9
disaster recovery, 23
general controls, 7-25
. access controls, 16
. categories, 7
. continuity of operations, 22
. control environment, 8
. controls over passwords, 20
. documentation, 25
organisational structure, 9
. physical access control, 17
. security policy, 16
. system development & implementation controls, 11-16
. system software & operating controls, 24
information system and internal control,4
mobile information and communication technology, 48-50
monitoring controls, 6
risk assessment, 5, 22

Chapter 9 – Computer audit- networks & related concepts
computer bureaux and audit implications, 26-27
computer environment at ProRide (Pty) Ltd, 30-35
databases, 9
. terminology, 9
. audit/control implications, 9
diagrams with/without EDI, 12-14
electronic data interchange (EDI), 11
. audit implications, 15
. risks/objectives, 15
electronic funds transfer (EFT), 16-20
. preventive, detective controls, 17-20
electronic messaging systems, 11
. benefits, 11
. risks, 11
Internet, 21-25
. email, trading etc, risks and controls, 22-25
networks, 5
. terminology, 5
. audit implications, 6
. access control, 6
. lan, wan, van, etc, 6
. security of communication, 7
ProRide computerisation, 30-35
trends in IT, 3
viruses,28-29
. audit controls, 29
. types, 28

Chapter 10 – Revenue and Receipts cycle
accounting aspects, 55
accounting system and control activities, 2
auditing the cycle, 54-73
auditor's toolbox, 57
basic functions of the cycle, 2
cash sale system, 40-42
characteristics of the cycle, 2
computerised revenue & receipts cycle, 20-39
control activities, 10-19
credit management, 5, 19, 35
documents in the cycle, 6
EFTs, 70
flowcharts for manual cycle, 7-19
financial statement assertions, 54
fraud in the cycle, 55
fraudulent financial reporting, 55
further audit procedures, 56
internal controls, 40-43
manual revenue & receipts cycle, 3-21
misappropriation of assets, 56
other audit procedures, 69
ProRide (Pty) Ltd revenue & receipts cycle, 44-53
significant risks, 57
substantive procedures, 59-72
tests of controls, 57, 58
window dressing, 71

Chapter 11 Acquisitions & payments cycle
Acquisitions and payments cycle – manual functions, 2-13
acquisitions & payments at ProRide (Pty) Ltd, 32
assertions, 42, 49 – 51
auditing the cycle, 41
basic functions, 2
. ordering, 2, 3, 7, 9
. receiving, 3, 7, 10
. recording, 3, 4, 7, 8, 11, 13
. payment, 3, 4, 8, 12, 13
computerisation – basic points, 14
. narrative description, 16 – 30
documents, 5
flowcharts, 6

Chapter 11 Acquisitions & payments cycle (continued)
fraud in the cycle, 42
further audit procedures
. overall response, 43
. tests of controls, 43, 44
. substantive procedures, 46, 47, 49, 52
ISA 315 (revised), 41, 44
ISA 330, 46
ISA 500, 43
internal control, 31
. control environment, 31
. risk assessment, 31
. monitoring, 31

Chapter 12 – Inventory & production cycle
accounting aspects for inventories, 18-20
assertions, 18, 24-27
auditing the cycle, 18-29
audit software use & procedures, 27-29
basic requirements for cycle, 3-4
. diagram basic requirements, 4
computers in the cycle, 13
cycle counts, 11-13
documents used in the cycle, 4-5, 12
financial statements/assertions, 2, 18
fraud in the cycle, 20-22
. inventory fraud, 3
. fraudulent financial reporting, 20-21
. misappropriation of assets, 21-22
IAS 2 – inventories, 18-20
inventory control at ProRide (Pty) Ltd, 14-17
inventory count attendance, 23
post inventory count procedures, 24
production, 8-10
. function, documents, risks, controls, 8-10
ProRide (Pty) Ltd – inventory control, 14-17
substantive procedures, 22
tests of controls, 22
warehousing, 6-7
. function, documents, risks, controls, 6-7
year-end inventory count, 12

Chapter 13 – Payroll and Personnel cycle
assertions, 38-39
auditing the cycle, 37-43
basic requirements of the wage system, 3
computerisation of the payroll, 14-28
documents used in the cycle, 5-6
EFT payments, 24-28, 33, 35
flowcharts for a manual wage system, 6-13
fraud in the cycle, 2,
further audit procedures, 39
internal controls, 9-13, 16-29
ISA 315 (revised), 37
payroll & personnel cycle at ProRide (Pty) Ltd, 31-36
ProRide payroll & personnel cycle, 31-36
risk assessment procedures, 29
salary system – manual and computerised, 29-30
wage system – manual, 3-13
wage system – computerised, 14-28
timekeeping, 3, 4, 7, 10, 19, 32

Chapter 14 – Finance and investment cycle
accounting system, 2
audit of the cycle, 6
auditing fair value, 7
audit procedures – finance cycle, 8
audit procedures – investment cycle, 18
characteristics of the cycle, 2
compensating controls, 3
debentures, 9
finance lease liabilities, 11

Chapter 14 – Finance and investment cycle (continued)
finance & investment cycle at ProRide (Pty) Ltd, 4-5
fraud in the cycle, 3
. fraudulent financial reporting, 3
. misappropriation of assets, 4
IAS 16 property, plant & equipment, 12, 18, 19, 20
IAS 17 leases, 12
IAS 32, financial instruments – disclosure, 25
IAS 36 impairment of assets, 23
IAS 37, provisions, contingent liabilities & assets, 14, 16, 18
IAS 38, intangible assets, 29, 30
IAS 39, financial instruments - recognition, 9, 25
ISA 315 (revised), 6
ISA 540 auditing accounting estimates, 7
ISA 620 using the work of an expert, 7, 27
investments in shares, 25
long-term loans, 5, 11, 27
property, plant & equipment, 18, 19, 20
risk, 2, 6
share capital & share premium, 8

Chapter 15 – Going concern & factual insolvency
auditor's objectives, 2
audit plan for going concern, nature, timing & extent 3, 4
audit conclusions, 6
audit risk, 2
Auditing Profession Act Sec 45, 9
auditing a subordination agreement, 10
auditor's report, 6
commercial insolvency, 8
common law fraud, 8
Companies Act Sec 22, 8
disclosure, 6
factual insolvency, 8, 9
financial indicators, 4
going concern assumption, 2
ISA 570 – going concern, 3, 4, 7
management plans, 5
mitigating factors, 5
operating indicators, 4
other indicators, 4
obtaining information about going concern, 3, 5
reckless trading, 8
reportable irregularity, 9
subordination agreements, 9

Chapter 16 – Reliance on other parties
audits of group financial statements (including work of a component auditor) 2, 3
auditor's expert – ISA 620, 2, 10-13
component auditors, 3, 4
documentation, 10
external auditors, 5, 6
internal audit function, 5-8
internal auditors, using their work ISA 610 (revised), 2, 5, 6, 8, 9
ISA 600, 2
ISA 610 (revised), 5
ISA 620, 10
King III report, 5, 6
nature, timing and extent, 11
other audit firms, 2
overall audit strategy, 3
reporting considerations, 5
responsibilities of group engagement partner, 3
risk assessment procedures, 3

Chapter 17 – Sundry topics
analytical procedures, 23
attorneys representation letter, 17, 18
audit documentation, 13
audit evidence, 16
auditor's report, 5, 9
duty of an auditor, 6, 7, 8
electronic confirmations, 20
events before, after and between financial statement and auditor's report, 5, 6, 7, 8, 10
external confirmations, 16. 19
initial audit engagements, 3
IAS 10 – events after reporting period, 5, 6
ISA 230 – using a service organisation, 25
ISA 500 – audit evidence, 16
ISA 505 – external confirmations, 16, 19
ISA 510 – initial audit engagements, 3
ISA 520 – analytical procedures, 23
ISA 550 – related parties, 11
ISA 560 – subsequent events, 5, 7
ISA 580 – written representations, 21
ISQ1 – quality control for firms that perform audits, 14
litigation and claims, 17, 18
related parties, 11, 12
reporting considerations, 4
SAAPS 4 – litigation and claims, 17, 18
SAAPS 6 – external confirmations from financial institutions, 19, 20
service organisations (using), 25
subsequent events, 5, 6, 7
written representations, 21

Chapter 18 – The Audit report
adverse opinion, 11
auditor's responsibility, 4
comments on structure and wording, 12
considerations before forming an opinion, 2
content of the report, 3, 9, 10, 11
directors' responsibility, 3
disclaimer of opinion, 9
emphasis of matter, 12
insufficient evidence qualifications, 6
ISA 706 – emphasis of matter, 12
ISA 710 – comparative information, 16
ISA 720 – auditor's responsibility relating to …
. inconsistencies, 18
. misstatements of fact, 19
material, 7
material and pervasive, 7
misstatement qualification, 6
modifying the audit opinion, 6, 14
modifying the audit report, 5, 14
objective of the audit report, 2
other matter paragraphs, 13
other reports required by the Cosact, 4, 19
qualification "except for", 9, 10
reportable irregularities, 15
report on other legal and regulatory requirements, 16
SAAPS 3 (revised) 2, 3
signing the report
structure of the audit report, 3
types of modified opinion, 8

Chapter 19 – Review engagements & related service engagements

Agreed upon procedures engagements – ISRS 4400, 17
. general principles, 17
. independence, 17
. objective, 17
. reporting, 18
. terms of engagement, 17
. types of procedure, 17
Compilation engagements – ISRS 4410 (revised), 19
. acceptance and continuance, 20
. association with false or misleading information, 20
. Companies Act 2008 requirements, 19
. definition, 19
. ethical requirements, 19
. independent accounting profession, 19
. objective, 19
. performing the engagement, 21
° practitioner's understanding, 21
° compiling the financial statements, 21
. professional judgement, 20
. public interest score, 19
. quality control, 20
. reporting, 22
. responsibilities for management, 20
Engagements to review historical financial statements -ISRE 2400, 2
. applicable accounting framework, 6
. comparison of an audit and a review, 3, 4
. companies which qualify for a review, 2
. conclusion: forming and expressing, 12, 13
. conclusion : modified, 13
: except for, 13, 15
: adverse, 13, 15
: disclaimer, 13, 15
. description of review engagement, 2
. ethical requirements, 5
. fraud and non-compliance, 11
. going concern, 11
. materiality, 7
. objectives, 5
. obtaining an understanding, 8
. pre-conditions for a review engagement, 6
. preliminary engagement activities, 6
. procedures
° inquiry, 9
° analytical, 9
° additional, 10
°reconciliation, 12
. professional scepticism, 5
. quality control, 5
. related parties, 11
. reportable irregularities, 4
. reporting, 13, 14
. review process, 7
. terms of engagement, 8
. written representations, 12