

Answers to Questions

1. When planning an IS audit, which of the following factors is least likely to be relevant to the scope of the engagement?

- A. The concerns of management for ensuring that controls are sufficient and working properly
- B. The amount of controls currently in place
- C. The type of business, management, culture, and risk tolerance
- D. The complexity of the technology used by the business in performing the business functions

Answer: B

The correct answer is B. How many controls are in place has little bearing on what the scope of the audit should be. Scope is a definition of what should be covered in the audit. What management is concerned about (A), what the management risk environment is (C), and how complex the technical environment is (D) could all have an impact of what the scope of a particular audit might be but not the sheer number of controls.

2. Which of the following best describes how a CISA should treat guidance from the IS audit standards?

- A. IS audit standards are to be treated as guidelines for building binding audit work when applicable.
- B. A CISA should provide input to the audit process when defensible audit work is required.
- C. IS audit standards are mandatory requirements, unless justification exists for deviating from the standards.
- D. IS audit standards are necessary only when regulatory or legal requirements dictate that they must be applied.

Answer: C

The correct answer is C. IS audit standards are mandatory to follow at all times unless justification exists for deviating from them. Complying with standards is one of the tenants of the IS Audit Code of Ethics and is not a guideline (A), does not apply only when the work needs to be defensible (B), or when regulatory or legal issues are involved (D).

3. Which of the following is not a guideline published for giving direction to IS auditors?

- A. The IT auditors role in dealing with illegal acts and irregularities
- B. Third-party service providers effect on IT controls
- C. Auditing IT governance
- D. Completion of the audits when your independence is compromised

Answer: D

The correct answer is D. When the perception of auditor independence is questioned, the audit management must investigate and determine whether the situation warrants actions such as removing the auditor or investigating further. There is no standard like the one mentioned, but the subject is covered in the organizational relationship and independence standard. The other answers are guidelines provided by ISACA.

4. Which of the following is not part of the IS auditors code of ethics?

- A. Serve the interest of the employers in a diligent loyal and honest manner.
- B. Maintain the standards of conduct and the appearance of independence through the use of audit information for personal gain.
- C. Maintain competency in the interrelated fields of audit and information systems.
- D. Use due care to document factual client information on which to base conclusions and recommendations.

Answer: C

The correct answer is C. Use of client information is unethical and a cause for revocation of your certification. The other three are tenants of the code of ethics.

5. Due care can best be described as

- A. A level of diligence that a prudent and competent person would exercise under a given set of circumstances
- B. A level of best effort provided by applying professional judgment
- C. A guarantee that no wrong conclusions are made during the course of the audit work
- D. Someone with lesser skill level that provides a similar level of detail or quality of work

Answer: A

The correct answer is A. Due care is a level of diligence applied to work performed. It is a reasonably competent third-party test. It does not ensure that no wrong conclusions are made (C) and is not related on a skill level (D) but a competence and prudence level. It is not a level of best effort (B). It is a benchmark to compare efforts against that which would have been done in similar circumstances by a prudent and competent person.

6. In a risk-based audit approach, an IS auditor must consider the inherent risk and

- A. How to eliminate the risk through an application of controls
- B. Whether the risk is material, regardless of managements tolerance for risk
- C. The balance of the loss potential and the cost to implement controls
- D. Residual risk being higher than the insurance coverage purchased

Answer: C

The correct answer is C. You do not want to eliminate risk (A), you want to only manage and control it. Managements tolerance of the risk is part of the definition of what is material so whether the risk is material (B) is not a correct answer. Insurance coverage is not necessarily the only control to consider for mitigating residual risk (D). The correct balance of cost to control any potential losses is a very important part of the risk mitigation considerations.

7. Which of the following is not a definition of a risk type?

- A. The susceptibility of a business to make an error that is material where no controls are in place
- B. The risk that the controls will not prevent, detect, or correct a risk on a timely basis
- C. The risk that the auditors who are testing procedures will not detect an error that could be material
- D. The risk that the materiality of the finding will not affect the outcome of the audit report

Answer: D

The correct answer is D. Answer A is the definition of an inherent risk, which is a risk in its natural state or without controls. A controls risk (B) is the chance that controls put in place will not solve the problem soon enough to prevent loss. A detection risk (C) occurs

when auditing does not discover material errors due to sampling or testing procedures.

8. What part of the audited businesses background is least likely to be relevant when assessing risk and planning an IS audit?

- A. A mature technology set in place to perform the business processing functions
- B. The management structure and culture and their relative depth and knowledge of the business processes
- C. The type of business and the appropriate model of transaction processing typically used in this type of business
- D. The companys reputation for customer satisfaction and the amount of booked business in the processing queue

Answer: A

The correct answer is A. All of the items listed are relevant, however, by itself the maturity of the technology has the least amount of bearing on the risk assessment of an organization. Just because it is a mature technology does not mean it is inherently risky or does not meet the needs of the business.

9. Which statement best describes the difference between a detective control and a corrective control?

- A. Neither control stops errors from occurring. One control type is applied sooner than the other.
- B. One control is used to keep errors from resulting in loss, and the other is used to warn of danger.
- C. One is used as a reasonableness check, and the other is used to make management aware that an error has occurred.
- D. One control is used to identify that an error has occurred and the other fixes the problems before a loss occurs.

Answer: D

The correct answer is D. While both are after the fact (A), the order of application is not really relevant. While corrective controls keep errors from resulting in loss (B), detective controls do not warn, deterrent controls do. While reasonableness checks can be a detective control, it also is used to make errors known (C).

10. Which of the following controls is not an example of a pervasive general control?

- A. IS security policy
- B. Humidity controls in the data center
- C. System-wide change control procedures
- D. IS strategic direction, mission, and vision statements

Answer: B

The correct answer is B. The other three are pervasive because they focus on the management and monitoring of the overall IS infrastructure. Humidity controls are specific to a single data center only.

11. One of the most important reasons for having the audit organization report to the audit committee of the board is because

- A. Their budgets are more easily managed separate from the other budgets of the organization
- B. The departments resources cannot easily be redirected and used for other projects
- C. The internal audit function is to assist all parts of the organization and no one reporting manager should get priority on this help and support
- D. The audit organization must be independent from influence from reporting structures that do not enable them to communicate directly with the audit committee

Answer: D

The correct answer is D. Independence from influence and for reporting purposes is the primary reason to have reporting lines outside of the corporate reporting structure.

12. Which of the following is not a method to identify risks?

- A. Identify the risks, then determine the likelihood of occurrence and cost of a loss.
- B. Identify the threats, their associated vulnerabilities, and the cost of losses.
- C. Identify the vulnerabilities and effort to correct based on the industrys best practices.
- D. Seek managements risk tolerance and determine what threats exist that exceed that tolerance.

Answer: C

The correct answer is C. The industrys best practices must be tempered by management tolerance for risk and their direction. The elimination of risks is not your goal. Risk is only relevant to managements

needs.

13. What is the correct formula for annual loss expectancy?

- A. Total actual direct losses divided by the number of years it has been experienced
- B. Indirect and direct potential loss cost times the number of times it might possibly occur
- C. Direct and indirect loss cost estimates times the number of times the loss may occur in a year
- D. The overall value of the risk exposure times the probability for all assets divided by the number of years the asset is held

Answer: C

The correct answer is C. Annual loss expectancy is the total losses both direct and indirect times the frequency of occurrence for that loss in a given year.

14. When an audit finding is considered material, it means that

- A. In terms of all possible risk and management risk tolerance, this finding is significant.
- B. It has actual substance in terms of hard assets.
- C. It is important to the audit in terms of the audit objectives and findings related to them.
- D. Management cares about this kind of finding so it needs to be reported regardless of the risk.

Answer: A

The correct answer is A. Materiality is a relative, professional judgment call that must take into context managements aggregate tolerance of risk, how this finding stacks up to all of the findings, and the potential cumulative effect of this error.

15. Which of the following is not considered an irregularity or illegal act?

- A. Recording transactions that did not happen
- B. Misuse of assets
- C. Omitting the effects of fraudulent transactions
- D. None of the above

Answer: D

The correct answer is D. None of the above is not an auditing irregularity or a possible illegal act based on the definition in the standard

16. When identifying the potential for irregularities, the auditor should consider

- A. If a vacation policy exists that requires fixed periods of vacation to be mandatory
- B. How much money is devoted to the payroll
- C. Whether the best practices are deployed in the IS environment
- D. What kind of firewall is installed at the Internet

Answer: A

The correct answer is A. While the others have varying relevance to audit testing, they do not indicate possible irregularities by themselves. A vacation policy that does not require staff to be away from work for a fixed period of time—usually one to two full weeks—enables employees to maintain fraudulent schemes without requiring a trained back up employee to step in and perform the process for at least some period of time during the year.

17. Some audit managements choose to use the element of surprise to

- A. Scare the auditees and to see if there are procedures that can be used as a back up
- B. Ensure that staffing is sufficient to manage an audit and daily processing simultaneously
- C. Ensure that supervision is appropriate during surprise inspections
- D. Ensure that policies and procedures coincide with the actual practices in place

Answer: A

The correct answer is A. Some of the other answers are nonsensical, but the real reason for using the element of surprise is to ensure that the policies and procedures documents line up with actual practices.

18. Which of the following is not a reason to be concerned about auditor independence?

- A. The auditor starts dating the change control librarian.
- B. The auditor invests in the business spin-off of the company.
- C. The auditor used to manage the same business process at a different company.
- D. The auditor is working as consultant for the implementation portion of the project being audited.

Answer: C

The correct answer is C. The fact that this was their job at another company may actually be an advantage for the audit team. The other items listed could lead to a compromise of the auditors independence and should be investigated.

19. Control objectives are defined in an audit program to

- A. Give the auditor a view of the big picture of what the key control issue are based on the risk and management input
- B. Enable the auditor to scope the audit to only those issues identified in the control objective
- C. Keep the management from changing the scope of the audit
- D. Define what testing steps need to be performed in the program

Answer: A

The correct answer is A. The scope is not defined exclusively by the auditor (C) and does not necessarily define testing the related tasks (D). Answer B is somewhat correct; however, Answer A is the best answer.

20. An audit charter serves the following primary purpose:

- A. To describe the audit process used by the auditors
- B. To document the mission and business plan of the audit department
- C. To explain the code of ethics used by the auditor
- D. To provide a clear mandate to perform the audit function in terms of authority and responsibilities

Answer: D

The correct answer is D. The charters main purpose is to define the auditors roles and responsibilities. It should evidence a clear mandate and authority for the auditors to perform their work. Unlike a mission statement (B) or a process document (A), it describes the bounds of authority. The code of ethics (C) is a nonrelevant answer to this exercise.

21. In order to meet the requirements of audit, evidence sampling must be

- A. Of a 95 percent or higher confidence level, based on repeated pulls of similar sample sizes
- B. Sufficient, reliable, relevant, and useful, and supported by the

appropriate analysis

C. Within two standard deviations of the mean for the entire population of the data

D. A random selection of the population in which every item has an equal chance of being selected

Answer: B

The correct answer is B. Sampling satisfies the evidence requirements that the data is sufficient, reliable, relevant, useful, and supported by the appropriate analysis. A random population section (D) is the definition of a random sample. Answers A and C do not make sense.

22. Audit evidence can take many forms. When determining the types required for an audit, the auditor must consider

A. CAATs, flowcharts, and narratives

B. Interviews, observations, and reperformance testing

C. The best evidence available that is consistent with the importance of the audit objectives

D. Inspection, confirmation, and substantive testing

Answer: C

The correct answer is C. The rest of the answers list types of audit evidence that could be considered, but the auditor must consider the best evidence available and determine what method for gathering and reviewing it as a second step in the audit planning process.

23. The primary thing to consider when planning for the use of CAATs in an audit program is

A. Whether the sampling error will be at an unacceptable level

B. Whether you can trust the programmer who developed the tools of the CAATs

C. Whether the source and object codes of the programs of the CAATs match

D. The extent of the invasive access necessary to the production environment

Answer: D

The correct answer is D. There is no sampling error with CAATs, which is one of their strengths (A), you will need to be aware of other participants in the process but that should be under your control (B), and understanding whether the source and object code

match is an issue with what you are testing not to itself (C). The best answer is that you should be concerned with the potential impact of your testing on live data.

24. The most important aspect of drawing conclusions in an audit report is to

- A. Prove your initial assumptions were correct.
- B. Identify control weakness based on test work performed.
- C. Obtain the goals of the audit objectives and to form an opinion on the sufficiency of the control environment.
- D. Determine why the client is at risk at the end of each step.

Answer: C

The correct answer is C. Answer A is not value-added to the client; neither is D unless there is a weakness identified first. Answer B is an okay answer, however, Answer C is the best possible choice.

25. Some things to consider when determining what reportable findings should be are

- A. How many findings there are and how long the report would be if all findings were included
- B. The materiality of the findings in relevance to the audit objectives and managements tolerance for risk
- C. How the recommendations will affect the process and future audit work
- D. Whether the test samples were sufficient to support the conclusions

Answer: B

The correct answer is B. Materiality, audit objectives, and managements direction are the key items to consider. Answer D needs resolving long before the findings are reviewed for reportability; Answer A, how many, or Answer C, the effect of the recommendations, is not an issue with whether they should be reported or not.

26. The primary objective of performing a root cause analysis is to

- A. Ask why three times.
- B. Perform an analysis that justifies the recommendations.
- C. Determine the costs and benefits of the proposed recommendations.
- D. Ensure that you are not trying to address symptoms rather than

the real problem that needs to be solved.

Answer: D

The correct answer is D. Answers B and C are not correct because they are related to recommendations and not to the root cause.

Answer A is a technique used in root cause analysis. The best answer is D.

27. The primary reason for reviewing audit work is to

A. Ensure that the conclusions, testing, and results were performed with due professional care.

B. Ensure that the findings are sufficient to warrant the final report rating.

C. Ensure that all of the work is completed and checked by a supervisor.

D. Ensure that all of the audits are consistent in style and technique.

Answer: A

The correct answer is A. The other answers are all important but the primary reason is one of ensuring due professional care by checking the work with a reasonably competent third-party review.

28. Which criteria would an IS auditor consider to be the most important aspect of an organizations IS strategy?

A. It includes a mission statement.

B. It identifies a mechanism for charging for its services.

C. It includes a Web-based e-commerce strategy.

D. It supports the business objectives.

Answer: D

The correct answer is D. While a mission statement (A) is certainly a common component of a strategy documentation, and charging mechanisms (B) can be included as a reference, the most important item to consider is the alignment of the strategy with the business needs and objectives. Web strategies (C) may or may not be relevant to the business at hand.

29. From a segregation of duties standpoint, which of the following job functions should be performed by change control personnel?

I. Verifying that the source and object code match before moving code into production

- II. Scheduling jobs to run in the production environment
- III. Making changes to production code and data when programs fail
- IV. Applying operating system patches

- A. I only
- B. I, II, and III
- C. II and IV only
- D. I and IV only

Answer: A

The correct answer is A. Scheduling jobs (II) would provide a change control person the opportunity to run jobs in combination with the changes they are applying, thus permitting potential fraud or the abuse of production processing. No direct changes to code or data (III) should ever be permitted by a nonprogrammer who is not acting on behalf of the application or user management. Job function IV could be seen as a change control function, but these systems level upgrades are typically applied by system programmers who are qualified to perform these functions and to ensure they are appropriately installed.

30. In a database management environment, which of the following functions should not be performed by the database administrator?

- A. Sizing table space and memory allocations
- B. Testing queries and consulting on table join limitations
- C. Reviewing logs for fraudulent activity or access errors
- D. Performing back ups and recovery procedures

Answer: C

The correct answer is C. Sizing database relevant components (A), testing queries and consulting on database access and views (B), and performing back up and recovery functions are all part of the DBAs job. They should not have the responsibility for reviewing audit logs (C) because they have access to modify the logs and are not independent from a capability standpoint. Although they can always change logs to cover up fraudulent activity, the role of review and the assurance that the logs are not tampered with by DBAs should fall to a supervisory position overseeing the DBA function.

31. Many organizations require employees to take a mandatory one to two full weeks of contiguous vacation each year because

- A. The organization wants to ensure that their employees quality of

life provides for happy employees in the workplace.

B. The organization wants to ensure that potential errors in process or irregularities in processing are identified by forcing a person into the job function as a replacement periodically.

C. The organization wants to ensure that the benefits provided by the company are fully used to enable full employment of replacement staff as much as possible.

D. The organization wants to ensure that their employees are fully cross-trained and able to take over other functions in case of a major disruption or disaster.

Answer: B

The correct answer is B. Employees in sensitive functions should be required to take at least a full weeks vacation annually to ensure that the opportunity for fraudulent or illegal activities are not perpetuated by their uninterrupted daily attendance to systems or processes. The other answers are all valid reasons for providing a job rotation or vacation requirement, but Answer C is the best answer from an audit perspective.

32. Which of the following would be most important in evaluating an IS organizations structure?

I. Human Resource policies that adequately describe job functions and duties sufficiently

II. Organization charts that identify clear reporting and authority lines

III. System configurations that are well documented in the system architecture

IV. Training requirements and provisions for cross training that are documented along with roles and responsibilities

A. I and II only

B. I, II, III, and IV

C. I, II, and IV only

D. II and III only

Answer: C

The correct answer is C. Important aspects of an IS strategy, of the items listed, include Human Resource policies, organization charts and clear authority lines, and training requirements. System configurations and architecture are not really related to the strategy of the organization but more to its system design than strategic direction.

While training (IV) requirements are not as important in a strategy document as I and II, it is still relevant and the best answer from an

audit perspective of those available.

33. In a review of Human Resource policies in an IS organization, an IS auditor would be most concerned with the absence of

- A. Requirements for job rotation on a periodic basis
- B. A process for exit interviews to understand the employees perception of management
- C. The requirement for employees to sign a form signifying that they have read policies
- D. The existence of a termination checklist requiring that keys and company property are obtained and all access permissions are to be revoked upon termination

Answer: D

The correct answer is D. The first three answers are good practices to be sure. But the revocation of access privileges and the ability to retain company assets and physical access to property is the most important item listed from an audit perspective.

34. A System Development Life Cycle can be best described as

- A. A process used by programmers to document SOP 98-1 compliance
- B. A methodology used to guide the process of software creation project management
- C. A system design methodology that includes all the steps in problem definition, solution identification, testing, implementation, and maintenance of the solution
- D. A process used to manage change control and approval cycles in a development environment

Answer: C

The correct answer is C. SDLC methodologies are described by all of the answers provided for this question to some extent. They can guide in change control and approval cycles (D) and the project management of software development. It also can be helpful when analyzing capital- versus expense-related tasks related to development projects, but Answer C best describes the SDLC components and use as a design methodology.

35. What is the primary difference between policies and standards?

- A. Policies provide a high-level framework and standards are more dynamic and specific.

- B. Policies take longer to write and are harder to implement than standards.
- C. Standards require interpretation and must have associated procedures.
- D. Policies describe how to do things and standards provide best practices guidance.

Answer: A

The correct answer is A. Policies are intended to be high-level guidance by senior management and should not change much over time, while standards are more technology specific and therefore may be more dynamic in nature. Policies are not necessarily harder to write or implement (B) and do not describe how to do things (D), those are called procedures. Policies may require interpretation and standards should be specific and clear for a given situation, which makes Answer C a wrong answer.

36. Which of the following is not a standard?

- A. Approved access control methodologies
- B. How to request a new account
- C. Minimum security baseline for hardening a UNIX server
- D. Description of acceptable back up and recovery methods for production data

Answer: B

The correct answer is B. How to request clearly spells out a step-by-step process to follow, which is better described as a procedure. Minimums (C), acceptable practices (D), and approved methods (A) all imply standards documentation.

37. Which of the following are not key considerations when reviewing third-party services agreements?

- A. Provisions exist to retain ownership of intellectual property and assets.
- B. The lowest price possible is obtained for the service rendered.
- C. Business continuity planning and processes are part of the signed agreement.
- D. Security and regulatory concerns are identified as risks during negotiations.

Answer: B

The correct answer is B. Lowest cost does not always mean the best

arrangement especially from a control standpoint. Ensuring that ownership is retained (A) for the intellectual aspects of the business that would be needed, should the business eventually go to another vendor, are very important to the survivability of the business. (C) BCP processes are an important part of any third-part relationship so alternatives are thought through and well documented before disruptions occur. Additionally, even though it is more important that security and regulatory concerns be addressed directly in the wording of the final agreement signed by both parties, identifying the issues in negotiations it is still more important than the lowest price from an audit and risk perspective.

38. When evaluating project management, which of the following would you be least concerned in seeing evidenced?

- A. Well-defined project scope and objectives
- B. Costs identified with the resources allocated to the project
- C. Timelines with achievable milestones
- D. Sponsorship and approval by business process management

Answer: B

The correct answer is B. All elements mentioned are important to a successful project and need to be set in place to manage the project successfully. In order of importance to the project, (D) sponsorship and backing is the most critical element, without which you cannot even get started. (A) Knowing where you are going through the scope and objectives also is clearly a key piece in managing anything. (C) Having a time frame documented to measure progress against is necessary to understand the comparative success against managements expectations along the way. (B) Knowing what the costs will be is important but may change through the course of the project, depending on needs to expedite certain sections and on the availability of resources. This can only be estimated throughout the project and only becomes good information after the costs are realized.

39. When evaluating a change control process, the IS auditor would be most concerned if he or she observed the following:

- A. Change control personnel permitting systems programmers to patch operating systems
- B. Computer operators running jobs that edit production data
- C. Application programmers correcting data errors in production
- D. Change control personnel copying code from the production for testing purposes

Answer: C

The correct answer is C. Programmers should never be permitted to directly access data in the production environment. Computer operators will initiate, by nature of their function, programs that may modify data (B). Systems programmers are permitted to patch systems and in fact, should be the ones performing this function (A).

The proper way to test production code is to first copy it from the live production environment to minimize the impact on the user community. No humans should ever directly manipulate the application code or data in the production environment.

40. During the review of a problem management system, it is determined that several problems have been outstanding and unresolved for an excessively long period. Which of the following reasons is most questionable to the IS auditor reviewing the management controls of this process?

A. The problem has been sent to the vendor who will send a fix with the next software release.

B. The problem has been determined to be a user error and has been referred to the business unit for correction and additional training.

C. The problem is intermittent and after researching, remains outstanding until reoccurrence.

D. The problem is seen as a low risk issue and is therefore low on the priority list to be addressed.

Answer: D

The correct answer is D. The first three answers are all legitimate reasons to have an outstanding problem on the tracking logs. However, problems can be misleading at first read, and it should never be assumed that because of the way a problem is reported, it is inconsequential. Many security breaches occur in this manner. Management should ensure that all problems are quickly investigated and their root causes are determined. The need to prioritize problems for addressing them implies larger volumes than the organization is equipped to handle, indicating other more severe control and management issues.

41. During the problem analysis and solution design phases of an SDLC methodology, which of the following steps would you be most concerned with finding?

- A. Current state analysis and documentation processes
- B. Entity relationship diagramming and process flow definitions
- C. Pilot testing of planned solutions
- D. Gathering of functional requirements from business sponsors

Answer: C

The correct answer is C. The other three answers are all part of a well-executed SDLC methodology used to design a system or software. However, the initial problem analysis and design phases of a development cycle are not the appropriate place for the testing of solutions, especially by piloting them with end users.

42. What is the primary concern that an IS auditor should consider when reviewing Executive Information Systems (EIS)?

- A. Ensure that senior management actually uses the system to monitor the IS organization.
- B. Ensure that the information being provided is accurate and timely.
- C. Ensure that the information provided fairly summarizes the actual performance of the IS organization so that indicators will be representative of the detailed tracking and monitoring systems.
- D. Ensure that MTBFs are kept to a minimum and within acceptable boundaries.

Answer: C

The correct answer is C. EISs must represent real-world information in order for them to be most useful to management. They must summarize the issues in production and enable management to get indicators of the underlying problems that need further investigation. Mean time between failures (D) is only one aspect of information monitoring. Having accurate and timely information (B) does not help if the information that is being reported is not the key indicator needed from which to best run the operation. It is up to management to use the system for it to be useful (A). Certainly, this is reflective of how well management is performing their function, but the quality of the information is the primary concern in a review of the system.

43. SOP 98-1 is an accounting position that needs to be considered by the IS auditor primarily because

- A. The AICPA requires all auditors to be aware and comment on this

statement of position.

B. Management may be capitalizing software development tasks that should be expensed.

C. Keeping track of development efforts from a capital and expense perspective is indicative of good management of IS organizations.

D. SOP 98-1 tracking systems are required to be interfaced directly to accounting systems and may introduce opportunities for fraudulent accounting.

Answer: C

The correct answer is C. The AICPA(A) provides this statement of position as guidance and does not, in general, require auditors to do anything unless it is required based on a risk analysis and professional due care. Although it would be a concern if management was not properly capitalizing development tasks (B), and this should be examined during the review, the use of this statement of position as an indicator of the management processes is the primary aspect of reviewing adherence to this advice. Direct interface with accounting systems (D) is not a hard requirement of this type of accounting method.

44. When reviewing the management processes for overseeing budgeting and spending, the IS auditor should be least concerned with which of the following items?

A. Ensuring that all spending is reconciled to a budgeted line item and the variances to budget are explained

B. Ensuring that all of the budgeted money is spent in a budget year

C. Ensuring that expenditures are recorded and reported on budgets to IS organizational management

D. Ensuring that SOP 98-1 provisions are adequately documented and appropriately allocated

Answer: B

The correct answer is B. Spending all budgeted monies is of little concern and in fact may be indicative of a well-run organization. The other three items are all relatively important to meeting the functional requirements of oversight and management of an IS organization.

45. When evaluating information security management, which of the following are not items the IS auditor would consider commenting on as a potential control weakness?

A. A security program had not been developed using a risk-based

approach.

B. The information security officer does not accept responsibility for security decisions in the organization.

C. The use of intrusion detection technologies has not been considered for use in the security program.

D. Account administration processes do not require agreement to acceptable behavior guidelines from all persons requesting accounts.

Answer: B

The correct answer is B. This question uses double negatives to confuse the CISA candidate. The answer is looking for the single item that is acceptable and would not result in an audit concern. Valid concerns include creating a security program without considering risk (A), not at least considering intrusion detection technologies (C) whether they are used or not depends on that analysis, and not making account users aware of their security accountabilities and responsibilities (D). It is not the position of the security management to own the security decisions in an IS organization and (B) it would therefore be considered an appropriate position for information security management to take. That accountability lies with senior management who make their decisions based on expert input from the security management as well as many other sources, including business, finance, human resources, legal, and so forth.

46. In evaluating business continuity management, what three factors are considered important aspects of the overall management of the program by the IS auditor?

I. Impact to the businesses has been studied and agreed to from the business management as a basis from which to understand the continuity needs.

II. Interactions of all affected processes have been identified so that priorities for recovery can be determined.

III. Recovery tests have been successful and determined to fully meet the needs of the business.

IV. Contracts have been negotiated with hot site vendors, enabling for the immediate declarations of disaster to result in quicker recovery times.

V. The procedures required to manage the business processes without the information systems have been well documented and moved off-site to provide for interim recovery processing.

A. I, II, and III

B. I, III, and IV

- C. II, IV, and V
- D. I, II, and V

Answer: D

The correct answer is D. Two of the items listed are not considered important aspects of all business continuity process management. Ensuring that recovery testing is successful (III) is not necessary and seldom the case in the real world. In fact, it takes constant testing and adjustments to get even close to a flawless recovery process execution, especially when actual scenarios are seldom what the testing scenarios were. Hot-site contracts (IV) may be applicable in some scenarios but certainly not all and are dependant upon risk tolerance and processing criticality and costs. The other items are required steps and a review of management would ensure that they are all part of the program.

47. Which of the following sets of documentation would an IS auditor expect to find at the off-site facility for business continuity and recovery processes?

- I. User manuals and training documentation
 - II. Current systems configurations
 - III. Current systems and application code
 - IV. Operational procedures and required forms and supplies for processing
- A. II, III, and IV only
 - B. I, II, and III only
 - C. I, III, and IV only
 - D. All of the above

Answer: D

The correct answer is D. In fact, there is more hard copy documentation that will be required to successfully recover from a complete loss of systems and personnel. Job descriptions, process flows, IS procedure manuals, interim security and control documentation, call lists and rosters, and production data up to the point of failure (to name a few) would all be required in hard copy should you have a need to recover the business from scratch.

48. The best way to understand the security configuration of an operating system is to

- A. Consult the vendors installation manuals
- B. Review the security plan for the system

- C. Interview the systems programmer who installed the software
- D. Review the system-generated configuration parameters

Answer: D

The correct answer is D, review the actual parameters generated from a direct query of the system. The system programmers (C) and the security plan (B) may give you information about the point in time when the system was installed, but patches and modification since that time may have significantly changed the current security since then. The vendors manual (A) will explain what your options are and may even recommend settings, but they have no bearing on the actual set up.

49. What three things are the most important security controls that should be present when reviewing an operating systems security?

- I. The code comes from a trusted source.
 - II. Audit logging is turned on.
 - III. Unnecessary services are turned off.
 - IV. The default passwords are changed.
 - V. Systems administrators do not have any more access than they need to in order to perform their job.
- A. I, II, and III
 - B. III, IV, and V
 - C. I, III, and IV
 - D. I, II, and IV

Answer: C

The correct answer is C. Audit logging does need to be turned on (II), but this is only effective when a process is in place to monitor and react to the logs. Systems administrators (V) should use their own account to perform their work, but these accounts will usually be patterned after the root account and the privileges will be very high. Attempting to limit their access is an exercise that adds little value to the risk mitigation process. Default passwords are the most common way for hackers to breach a server (IV) and are very important to change. Any services that are not being used also should be turned off, because they are another common attack avenue (III). Any of the primary security checks would ensure that the code is trusted and has integrity to begin with (I).

50. Databases are complex to evaluate from a risk perspective because

- A. Access controls for application views, query permissions, field

level table access, as well as access to reports and query results must be reviewed to assess the security of data.

B. They can have complex data structures that may be joined through several keys.

C. Data definitions must be maintained in order to understand the data classifications.

D. Data flows and data normalization processes make both table sizing and transaction mapping difficult.

Answer: A

The correct answer is A. Risk is introduced when users have access to data that they have no rights to access. This is very difficult to prevent when so many ways exist to get access to the data that should be protected. Definitions, structures, and flows are important to understanding how the database is meant to operate and whether it will function efficiently, and unless they are seriously flawed, they will not add material risk to the IS organization.

51. In a two-phase commit database transaction, the roll back process is initiated

A. When the client and server cannot agree on a communication protocol

B. In multi-tier architectures that need to reject a proxy request

C. When a committed transaction cannot be completed by all participating servers and clients involved

D. When ownership of the session cannot be assured and committed to

Answer: C

The correct answer is C. In a two-phase commit process on multi-tier client server architectures, transaction processes negotiate a transaction through a commit process that locks data and notifies all of the parties of the intention to process the transaction. If for some reason, this cannot be accomplished to the satisfaction of all involved parties, the roll back process puts everything back to where it was before the transaction started. The other answers are nonsense.

52. Which of the following is not a design consideration to investigate when reviewing security packages?

A. What kind of changes and compromises must occur to existing processes

B. How well the security updates and patches are maintained on

the security package

C. What weaknesses and deficiencies cause a security package to be considered

D. What kind of support effort will be required to maintain the product adequately

Answer: B

The correct answer is B. The changes and effects of implementing a security package (A) must be part of the design consideration so they can be accommodated in the new processes. Similarly, the additional support effort, which is necessary for the product, must be considered in the design as well (D). The weaknesses that caused a security package to be considered in the first place (C) will be your primary design consideration. How well patches are maintained (B) is not a design criterion, but rather it pertains to how well the maintenance of the system is being performed.

53. Which of the following is not normally a concern when reviewing the implementation of an operation console system?

A. Whether the expertise to implement the system is being provided by the vendor to backfill existing functions, enabling the existing staff to learn the new systems

B. Whether the scope and goals of the implementation plan are being met in a cost effective and timely manner

C. Whether the KPIs used to manage the business will be improved by the implementation process

D. Understanding how well the console will interface with other operations components and what compatibility issues exist

Answer: C

The correct answer is C. KPIs are not an important implementation concern but rather are related to the use of the tool after it is installed and working. Knowledge transfer (A), scope creep, cost and deadline overruns (B), and interface issues (D) will be the major issues with this kind of implementation.

54. Which of the following will not be information that you would expect to find documented when evaluating a computer hardware installation project?

A. Procedures for defining the requirements and submitting the requests for proposals and bids

B. How the hardware installation has improved the process

throughputs

C. Functional requirements for the hardware based on the business plans and needs

D. Placement and location decisions for equipment installations

Answer: B

The correct answer is B. How the process has improved the throughput is something that can be predicted and planned for, but actual results will not be available during the planning and installation of new hardware. The other items need to be evidenced with good documentation.

55. Which of the following is the most effective method of assessing the controls over the hardware maintenance process?

A. Look at the hardware and assess whether the maintenance is current and that the equipment is well kept.

B. Following the recommended maintenance tasks and maintenance schedules, determine that the procedures are carried out and evidenced as completed by logging and dating the actual maintenance efforts.

C. Identify the required maintenance procedures from the vendors information and ensure that these processes are addressed by the IS organizations procedures.

D. Look at the problem logs and validate whether maintenance processes are determining the mean time between failures when compared to the industry averages.

Answer: B

The correct answer is B. The best way to ensure that maintenance processes are in place is to look to a control that evidences the actual completion of the recommended maintenance procedures. Observing hardware conditions (A) will only tell you about most recent activity, not historic behavior. Just because the right procedures are in place (C), you cannot be assured that they are carried out in practice. Just because there are not problems (D), you cannot assume that maintenance is being performed properly.

56. When reviewing voice systems maintenance processes, which of the following is the least critical to the audit objective of ensuring customer satisfaction?

A. Ensuring that as-built drawing modifications are made to the copy of the drawings kept in the office

- B. Ensuring that the support staff is knowledgeable and available to perform the necessary maintenance tasks
- C. Ensuring that the physical security of the PBX devices is managed properly
- D. Ensuring that planning and configurations provide for flexibility with minimal impact to the user base

Answer: A

The correct answer is A. Having knowledgeable and available staff (B) is very important to customer satisfaction. Ensuring that designs can change (D) without impacting the users also is important, too. Physical security can prevent malicious behavior that will affect the throughput of the system (C), but a built drawing in the office will have direct and little impact on customers. This is especially the case if built changes are noted in the field copies of the drawings, which is usually where you will find these changes noted. Field drawings should always be consulted as the working copy of what is actually in place.

57. Which of the following should an IS auditor review when performing an assessment of a PBX?

- I. Ensure that the dial-in numbers enabling toll-free outbound access are turned off.
 - II. Ensure that voicemail systems do not enable access to phone lines through hijacking.
 - III. Ensure that the access codes for the maintenance ports have been changed from the default.
 - IV. Ensure that outbound toll numbers, such as 900 numbers, are restricted.
 - V. Ensure that excessive phone usage is flagged and investigated for fraud.
- A. I, II, III, and IV only
 - B. II, III, and IV only
 - C. II, III, IV, and V only
 - D. I, II, III, IV, and V

Answer: C

The correct answer is C. All of these answers except (I) are necessary activities for a PBX review. Voicemail systems (II) need to be contained to mail traffic only and the ability to use these access points to the system to get a dial tone should be controlled and not enable any hijacking to occur. Access codes for maintenance ports (III) should be strictly controlled and not only changed from their vendor given

defaults but changed periodically. 900 numbers and other outbound toll scenarios (IV) should be controlled, and the business decisions should support any allowance for these costs to be incurred. Any excessive call tolls (V) outside of a predetermined boundary should be immediately flagged as potentially fraudulent and investigated if not shut down until an investigation can occur. The ability of obtaining an outbound toll-free line from a dial in number (I) is a business decision and may be turned off, but that is a risk and business decision that should be made by management not the IS auditor. The audit should verify that this is a conscious decision of the business, however.

58. Which of the following would you not expect to find in an Internet DMZ?

- A. DNS servers that advertise addresses to the Internet
- B. Mail relay servers that receive incoming mail and push outgoing mail
- C. Web servers containing content and business logic
- D. Proxy servers that authenticate access requests to internal content

Answer: C

The correct answer is C. You would never want to place your business logic in a DMZ where it could become vulnerable to the Internet. This exposes your logic to hijacking and alterations that may provide an avenue for a hacker to get inside the secure domain. The other items you would expect to see in this neutral area and acting as intermediaries. It is assumed that the DNS servers would advertise to internal addresses but only those in the DMZ to the Internet.

59. When reviewing data network architecture, which of the following is not a primary review criteria for the IS auditor?

- A. All router access is controlled by secure authentication methods.
- B. Network routing enables for the efficient flow of the businesses critical traffic.
- C. Protocols that are not needed for the business and administration of the network are disabled.
- D. VLANs using layer 2 switching techniques are employed to secure the traffic of critical data.

Answer: D

The correct answer is D. The other three issues should always be reviewed when assessing a data network, but layer 2 VLANs are a

special case that will be deployed only in certain situations and will not be assessed unless the business case calls for their use.

60. In a well-segregated operational environment, which of the following scenarios would you expect to see?

- A. Computer operators responding to systems messages and initiating problem tickets for failed jobs
- B. Change control librarians making modifications to code only when notified of errors by the application programmers
- C. Tape librarians managing print queues and reloading paper for printers as well as loading off-site storage containers with back up tapes
- D. Operators assisting system programmers with troubleshooting the operating system by adjusting parameters while the programmers observed the results

Answer: A

The correct answer is A. This is a properly set of functions that restrict the operator to the role of response and notify. In Answer B, the librarian is making changes to code, which should not be allowed, even if he or she is asked to do so. In Answer C, the librarians have access to both the beginning and end of a process, thereby enabling them to control a process that is not intended. In Answer D, the operator is making changes and should instead support this effort by doing the observation instead of making the change.

61. What are the most important criteria to assess when reviewing job descriptions?

- A. The job functions are all defined for the work that needs done, and training is required
- B. Clear authority is established and everyone knows who holds what roles in the organization
- C. Vacations are mandated and job rotation is provided for
- D. Performance is monitored and raises are based on goals that are defined jointly

Answer: B

The correct answer is B. Clear authority and all jobs with an owner are the most important aspects of the job description review. The other items also are important to have, but without clear lines of authority there is no way to enforce the other issues in the first place.

62. The primary purpose of key performance indicators is to

- A. Give management the ability to make sure that the staff is doing their work
- B. Monitor the capacity of the systems equipment and process performance metrics
- C. Provide management with a tool to gauge the overall health of the process and to point to potential trouble spots
- D. Enable operators to know when things are going wrong and whether the SLA is being met

Answer: C

The correct answer is C. KPIs are meant to be a tool for management to get a pulse on the operations quickly and at a glance. They should enable the subsequent drill down to more data, which will better explain the indications provided at a high level by the KPIs. The other answers are not correct.

63. In a media management system review, the IS auditor does not need to concern themselves with

- A. Whether the systems catalog accurately reflects the physical library's location of the media
- B. Whether the media is accessed by only those individuals with a need to know.
- C. Whether the media is accurately identified for movement off-site for back up purposes
- D. Whether the system adequately retires media and provides for its recycling in a secure manner

Answer: B

The correct answer is B. While this is an important concept in general, it is not the design of the media management system to ensure that access is properly controlled to the data. This is typically the functionality of the security management system. The media system does ensure that the correct jobs request the data, but it makes no decisions on need to know. The other answers are part of the expected functionality of a media management system.

64. What is the most important aspect of a change control system?

- A. All changes are documented and approved.
- B. Changes are managed through automated tools, preventing

access from people.

C. Copies of production are maintained in case the change fails.

D. Quality is ensured through testing and approval.

Answer: A

The correct answer is A. All changes must be recorded and approved in order for a change control system to be any good. Automated tools are nice (B) but not a requirement. Copies can be maintained (C), but any valid back out procedure will do and QC and testing processes (D) are only tangentially tied to a change control process and are not necessarily part of that process.

65. When emergency changes are identified during a change control review, what should the IS auditor also expect to find?

A. A control weakness, because these actions should not be allowed to occur and it should be reported

B. That the changes were applied as necessary and the related problems tickets were logged

C. Disciplinary actions related to enabling the changes to occur without approval by the system owner

D. A process for notifying the system owner of the changes and all associated actions taken with explanation.

Answer: D

The correct answer is D. Emergencies happen. Access needs to be permitted for fixes when required. This reduces your possible responses down to Answers B or D. Answers A and C are out of line. Answer B is incorrect because there is no provision for notifying the owner (or approver) that a change was allowed without their approval.

66. Which characteristics of a problem management system are important to the IS auditors review?

I. All problems are tracked through to conclusion.

II. All problems are initiated automatically, thus ensuring that the correct data is captured.

III. Escalation processes ensure that problems do not sit unresolved.

IV. All relative IS operation areas have access to the system to review and address the problems.

V. Statistics can be gathered from the system to facilitate the analysis of the IS problems.

A. I, II, III, IV, and V

B. I, III, IV, and V only

- C. II, III, IV, and V only
- D. I, III, and V only

Answer: B

The correct answer is B. All of these items except for item II are most important. Item II cannot be implemented practically for all problems. There will always be problems that will be identified and will not originate from automatic sources. These problems also will need to be entered into the management system, and tracked and resolved.

67. Critical aspects of an SLA review include all of these items except
- A. An annual review and re-validation of the business needs
 - B. Ensuring that the expected services are clearly defined
 - C. Ensuring that monitoring and escalation procedures are in place
 - D. Ensuring that the service provider is supplying service to all customers equitably

Answer: D

The correct answer is D. This issue should not be of concern to an individual agreement between one provider and one client. How the provider treats other customers is not part of the agreement being reviewed. The other answers are and should be evaluated.

68. What is the most important aspect of performing an evaluation of information security controls on a process or system?
- A. Ensuring that the best practice control techniques are being utilized properly
 - B. Understanding the businesses functional requirements of the process to ensure that they can be accomplished
 - C. Ensuring that the deployed controls work as part of the overall security architecture program
 - D. Making sure that access is strictly controlled based on a need to know

Answer: B

The correct answer is B. Best practice control techniques properly utilized (A) will need to be applied relative to the business needs, and they cannot be deployed without considering the goals of the business and the security control parameters that the business process places on the system. It also is important to ensure that the security controls used work well together and compliment other controls used in the architecture providing defense in depth (C), but not without first considering the business goals to ensure the

business needs are met. Restricting access based on a need to know (D) also is an important concept and will be a secondary step to ensuring access control that will follow from first understanding the business needs. Those needs define the need to know for the systems users.

69. The concept of data integrity implies that

- A. Access has not been given to those who do not have a need to know
- B. Data can be accessed by processes when necessary to support the business function
- C. Data has not been altered or modified outside of the expected and approved processing steps
- D. Data has not been made available to processes for which the data classification has not been accredited

Answer: C

The correct answer is C. Integrity implies that the data has not been altered from its intended state. Confidentiality is the concept that relates to access control (A), based on data classification (D), and availability is the concept that is used when referring to the data being accessible when needed (B).

70. When reviewing security and business risks, it is most important to keep in mind that

- A. Business risks are not as important as the security exposures to potential hackers.
- B. The customers expectation of privacy should take precedent over the businesses risk tolerance when considering security controls.
- C. Data classification should determine the security controls requirements.
- D. Some compromise of the security controls to accommodate the businesses risk tolerance is a necessary part of doing business.

Answer: D

The correct answer is D. The compromise of security to meet the business needs is a necessary part of doing business in the first place. Without taking risks, there would be no profit margin. The tolerance for the risks taken by the business is the primary security constraint, secondary only to the legal requirements, which may even be arguable. Certainly risks related to hackers (A) should be

one of the business risks considered for security controls, but it does not solely define the business risk. Customer expectations (B) should be important to businesses that want to keep their customers, but this does not take precedent over the business risk tolerance. Data classification is important (C), but it is the outcome of a business risk decision process, not a driver.

71. When evaluating the role of the information security officer, you should be most concerned to find that

- A. The security officers role was not well documented as part of the job description.
- B. The security officers role is defined as a key decision maker on a new product review committee.
- C. Part of the defined role was the accountability for ensuring that the security controls kept any security breaches from occurring.
- D. The authority for carrying out the role of a security officer was not explicitly tied to the organizations policy.

Answer: C

The item that should cause the most concern to the IS auditor will be Answer C, the expectation that all security breaches can be prevented. This is not possible to accomplish and the security officer will not be successful with this mandate. Poorly defined roles (A) and unclear lines of authority (D) can be corrected and adjusted to bring them in line, but an expectation to solve the security concerns completely is unrealistic. Participating on a product review committee is an appropriate role for an information security officer.

72. When reviewing an information system to assess its privacy risks, an IS auditor would consider all of the following except

- A. Ensuring that the appropriate consent has been obtained from the customer before the release of sensitive data
- B. The business needs for the client data within the processes
- C. Proper disclosures to the customer of what the data is used for and how it will be protected
- D. The laws and regulations relevant to the industry for privacy controls on customer data

Answer: B

The correct answer is B. The business needs are not related to the

privacy risk because they are the original purpose for gathering the data and presumably the one purpose for which the client approves the data be used. Consent (A), disclosure (C), and most importantly the regulations related to the business sector are definitely part of the risk equation. Note: Resale value was originally going to be put in as the wrong answer, but upon reflection the author realized that the value of the data to others is potentially part of the risk assessment and should be considered when determining control needs.

73. While reviewing an information security program the IS auditor determines that the best practices have not been followed as guidelines for developing the program. Which of the following would be the least important factor to consider when determining the recommendation related to changes for the program?

- A. Whether a risk assessment was part of the determination of what the program elements should be
- B. Whether the security officer had documented policies and procedures to direct the program
- C. Whether the architectural design of the security deployed an in-depth state-of-the-art defense
- D. Whether any inventory of the existing controls for managing security threats has been done

Answer: C

The correct answer is C because state-of-the-art defense in-depth cannot be determined without first looking at the other three answers and additional issues as well. Risk assessments (A), which used the inventories of the existing controls (D), threats, and vulnerabilities, are necessary steps to developing a security program and may preclude many best practice elements, depending on the assessments outcome. Of course, policy and mandate from the top of the organization (B) is a necessary first step to the program existing at all.

74. Policy for information security is a primary requirement for establishing control in an IS organization. Which of the following is not a reason why this is the case?

- A. A policy establishes the steps required to put security in place.
- B. A policy establishes the authority and accountability to get the security job done.
- C. A policy sets the expectations for the employees behavior as it relates to security.

D. The policy provides the mandate for putting the security program elements in place.

Answer: A

The correct answer is A. Policies are not meant to describe step-by-step processes, which are called procedures. Security policy establishes the authority (B), the management expectations (C), and the mandate for the program (D), but the actual implementation is to be interpreted from the high-level policy.

75. During an IS audit, the IS auditor determines that there is a control weakness due to the lack of available standards. When developing the findings and recommendation for the audit report, which of the following items should not be considered for inclusion as reasons for improving standards in the organization?

- A. Standards provide common ground that will increase the efficiency of the operations
- B. Standards creation is an industry best practice
- C. Standards ensure that individual policy interpretation will not result in the establishment of weaker security overall by lowering the minimum security level
- D. Standards provide simplified solutions to problems, enabling leverage of fewer solutions and economies of scale

Answer: B

The correct answer is B. Just because they are the industry's best practice is not a good reason to recommend that they be implemented. Management wants to see a value-added recommendation and is not as interested in keeping up the industry's latest fashions. Efficiency (A) and economies of scale (D) are important drivers to management and should be offered as benefits of improving controls whenever possible. Establishing a floor for security (C) also is very important but may need a little more explanation to management to sell the concept.

76. During your review of an information security risk assessment, which of the following elements would you be least concerned with if no evidence was available to substantiate it?

- A. The exercise of risk assessment is re-performed periodically.
- B. The threats and vulnerabilities have been determined.
- C. The existing controls have been inventoried and assessed for effectiveness.

D. The risk assessment included a tactical as well as a strategic initiatives assessment.

Answer: D

The correct answer is D. Tactical and strategic relate more to the resolution of the issues than it does to risks. Assessing risks identifies exposure to bad things happening. It identifies the loss potential and is determined by understanding the threats and vulnerabilities (B), the existing controls in place (C) to manage these threats and vulnerabilities, and should be periodically re-performed (A) to identify changes in the other elements and to reassess the overall risk.

77. When making a recommendation to establish a product review process that includes the security officer as part of the approval team, what should your strongest argument in the recommendation be?

- A. Security that is built into a process as part of the initial design can be seven times cheaper than the cost of implementing it after the product is in production.
- B. Plans should be documented and defended to upper management before they are used to implement a new program.
- C. The return on investment for products should be assessed prior to starting development so that these returns can be compared to actual gains after the product has been implemented.
- D. Plans should be evaluated to ensure that they follow the SDLC methodology standard in the organization and that the methodology has input from information security.

Answer: C

The correct answer is C. Return on investment is the strongest case that you can make to management and is the primary reason for performing this preliminary assessment if it is not in place. Security controls (A) is secondary to the business needs as is the planning methodology (D) or the plan documentation (B).

78. When reviewing the identification process used to establish user accounts, what is the most important aspect of the process?

- A. All of the relevant information is gathered about the person establishing the identity.
- B. Proof is provided to strongly tie the individual presenting themselves as the person for whom the ID is being established.
- C. Authorization is obtained for all accounts provided for the individual

who is requesting access.

D. The individual is given the opportunity to change their password immediately upon first log in.

Answer: B

The correct answer is B. Tying an actual person to the ID or account is the key factor in the identification process and is what establishing identity is all about. Gathering relevant information is an important administrative function (A) and the authorization processes should always include approvals (C). Good authentication processes will always enable users to create their own password (D) to ensure their identity is maintained, however, establishing identity requires proving you are who you say you are.

79. The security concept of need to know implies all of the following except

A. All access allowed within a permission set or role that is approved on a need to know basis can be viewed, copied, or modified because of the permissions granted.

B. Access is required to perform the assigned functions supporting the business process.

C. Data owners and their stewards have explicitly determined that the access by this role or person is acceptable.

D. The least amount of privilege necessary to perform the function has been granted to the role or person receiving this permission.

Answer: A

The correct answer is A. Just because permission has been granted does not mean access within the permitted range is acceptable at all times. Privacy considerations and ethical behavior should take precedence over permissions in situations where broader access, which is necessary for a particular function, is granted to the individual overall. Certainly being granted access implies that this access may be needed in order to perform the function for which it was permitted (B) at some point in time. And the implication is that that permission was a decision made by the data owner or their designated steward (C). It also implies that a least privilege methodology (D) was used to determine what access should be permitted and what should be denied.

80. An IS auditor would expect to see a defense in-depth approach to security or would recommend that one be adopted for all of the following reasons except

- A. It provides several different security mechanisms that increase the difficulty for hackers and intruders due to the increased knowledge required for compromise.
- B. More complex security solutions can lead to higher requirements for training and related support costs including audit requirements.
- C. Security solutions never completely solve a problem and a defense in-depth approach provides opportunities to address residual risk from one solution with another solution.
- D. Costs can be reduced by multiple iterations of solving most of a problem at a minimal cost and then applying another economic solution to address most of the remaining exposure rather than the extensive and expensive application of one solution set.

Answer: B

The correct answer is B. The one downfall of a defense in-depth solution approach is that it can increase training and maintenance costs. It does, however, provide many benefits that can outweigh this issue, if it is planned and deployed properly. The increased complexity is a barrier to attackers (A) and can provide for a more complete security solution (C). It also can be more economical than trying to solve a problem completely with one solution (D) and the savings could easily overcome the increased costs in training and maintenance.

81. When reviewing role-based access, which of the following parameters should the IS auditor be least concerned with?

- A. Business functions and job descriptions provide the input to determine that the accesses defined are sufficient to performing the required tasks.
- B. The defined role is applicable to a job function or set of job functions that provides a categorization of need that defines a role.
- C. The access permissions of a particular role are reconciled to the actual functions performed on a periodic basis.
- D. The establishment of new roles is reviewed and approved by the data owner or steward.

Answer: B

The correct answer is B. This is the least important of these aspects of the role-based access definition. From the users perspective, the role must be relevant and inclusive of the functions to be performed (A). These permissions must be periodically reviewed and validated (C) and changes have to be approved by the data owner to preserve the classification of data that they established (D). Whether these

roles are unique to a particular user or applicable to a large number of users is the least important issue.

82. During an evaluation of an account administration process, what should an IS auditor be most concerned about finding?

- A. Employee terminations that did not result in the closing of computer accounts in a timely fashion
- B. Time-of-day restrictions that were not used to limit access to systems
- C. Password aging that was not forced on accounts providing access to the network
- D. Accounts, which were supposed to have been suspended from disuse, were not followed up on and deleted

Answer: A

The correct answer is A. Closing computer accounts for those who no longer have a need to know puts data at risk more than the other situation mentioned here. Time-of-day restrictions (B) is an additional constraint, which can be applied to an account that would otherwise have access to the data, and is therefore not a strong control. Password aging (C) is a best practice, but strong passwords may mitigate the risk of not aging the passwords. Closing suspended accounts (D) is a good practice and there is some risk that they could be reopened either inadvertently or through social engineering, but this risk is primarily a housekeeping concern.

83. When evaluating a single sign on implementation, what single factor adds the most risk and provides concern for the IS auditor in their review?

- A. The fact that password resets must be effectively propagated across all systems in some way for single sign on to work properly
- B. The issue of systems administrators making changes to a system managed by the single sign on solution, thus putting the accounts out of synchronization
- C. The concern that single sign on cannot be effectively achieved unless roles and access needs are defined for all systems on which the user may need to perform their functions
- D. The concern that, if compromised, the single sign on access provides a wide range of access where access had been more limited previously

Answer: D

The correct answer is D. Aggregating access through a single key or

access point gives only one defense point to many security requirements that were provided separately prior to the single sign on solution. The inconvenience experienced by the users was the trade-off to more security and now being more convenient, there is less control in place. The other issues are important considerations for the implementation review but do not add the highest risk to the implementation.

84. When reviewing application design processes for information security controls, which of the following is least likely to be of concern to an IS auditor?

- A. The SDLC methodology does not require that security is considered as part of the design criteria.
- B. The testing of the application coding does not consider the security requirements identified in the design phase of the systems development process.
- C. The sample data used for testing and design is not adequately segregated from the production version of the data.
- D. Access permissions of testing and design personnel permits data modification in the test environment.

Answer: D

The correct answer is D. Access permissions during design and testing are the least concern of the items listed here. A process should be in place that ensures that the permissions are not carried through to the production environment, however. The highest concern would be (A) no requirement for security in the design phase. Without this consideration, testing for that design input (B) would not be possible. There also are concerns with production data mixing with test data, because live production data integrity could be negatively impacted.

85. Which of the following are data classification controls?

- I. Labeling the removable media containing classified data with the highest level of data sensitivity contained on the media
- II. Publishing a policy that defines what data classifications are and how these classifications are to be applied
- III. Encrypting data when it is being transmitted across the Internet
- IV. Treating all forms of a given data classification as equal in terms of protection requirements
- V. Regulatory requirements to protect customer data from disclosure without prior consent

- A. I, II, and IV only
- B. I, II, III, and IV only
- C. I, II, III, IV, and V
- D. I, II, IV, and V only

Answer: B

The correct answer is B. The only item listed here that is not a control at all (V) is a requirement that does not constitute a control all by itself. The other items are controls that may be put in place to help ensure this requirement is met, but requirements are not controls

86. Which of the following is not a password control?

- A. Requiring that a password have a minimum length and complexity
- B. Encrypting passwords when in transit and at rest
- C. Limiting the reuse of passwords through the use of a history file
- D. Limiting the number of unique sessions an account can initiate

Answer: D

The correct answer is D. The number of times an account can create a unique session is an account control and is not related to password controls. The other items are controls that may be applied to passwords.

87. When evaluating strong authentication usage, what should an IS auditor be most concerned with?

- A. Ensuring that the two factors are maintained in separate databases to ensure segregation
- B. Determining the identification process for each factor and ensuring they are synchronized
- C. Reviewing the biometric aspects of strong authentication or acceptable type I and type II error rates
- D. Reviewing the physical controls related to the storage of the physical tokens or card stock supplies

Answer: B

The correct answer is B. The IS auditor should be most concerned with the matching the identity of the actual user to the various authentication factors. Keeping the various factors separated (A) should not be a consideration at all; in fact, it may be better to secure them simultaneously. Type I (false rejection rate) and type II (false acceptance rate) would be important factors to consider if biometrics were involved, but that is not a criteria in the question. Many strong authentication solutions do not use biometrics as part of the solution. The physical

security of a token or card stock not yet issued should be of lesser concern than ensuring that the users identity has been matched up to the various authentication factors. Again, hardware devices may not be part of the strong authentication solution being evaluated.

88. During a review of a PKI, the IS auditor determines that nonrepudiation cannot be assured for a set of transactions. This most likely means that

- A. The certificate authority will not stand behind the validation of the certificate used at the time when the transaction occurred.
- B. The users certificate was compromised or was expired when the time the transaction occurred.
- C. In reviewing the transaction flow and the security related to the use of the certification, it cannot be conclusively proven that no other person could have possibly been responsible for the transaction that had occurred.
- D. The transaction did not go through as anticipated, causing a roll back of the request and negating the signed transaction.

Answer: C

The correct answer is C. Non-repudiation implies proof that your request came from you and no one else. There are several reasons why this may be the case, which may include a CA defaulting on their responsibility (A), or a compromise or expiration of the certificate (B). Transaction roll back (D) is not associated with non-repudiation at all, and if it were to occur, there would be no need to prove a transaction.

89. Which of the following would an IS auditor expect to see as part of an information security architecture?

- I. Evidence of the application of a defense in-depth strategy
 - II. A risk-based approach to the application and location of the security controls
 - III. A plan that takes into consideration the business needs and processes
 - IV. The inclusion of the management and operational controls as well as technical controls
- A. I, II, and IV only
 - B. I, II, III, and IV
 - C. II and IV only
 - D. I, II, and III only

Answer: B

The correct answer is B. All of the items listed should be found in comprehensive security architecture.

90. When performing a review of the host-based security controls, the risk factors that need to be considered are

- I. The value of the data contained on the server being secured
 - II. The functions and tasks required of the server
 - III. The services that are not needed in the configuration of the server
 - IV. The operating system type and its vulnerabilities
 - V. Requirements for encryption related to the services provided by the server
- A. I, II, III, IV, and V
 - B. I, II, and IV only
 - C. II, III, and V only
 - D. III, IV, and V only

Answer: B

The correct answer is B. These three items are factors that may introduce risk, operating system type, business needs, and the value of the data. Services that are turned off do not constitute any risk at all (III). Requirements for encryption do not introduce risk unless, of course, this requirement is addressed in a less than optimal fashion.

91. Minimum security baselines (MSBs) and host-based intrusion detection relate to each other in what important aspect?

- A. They both are security controls that apply to a device (server) as opposed to network-based controls.
- B. Host-based intrusion detection cannot be successfully implemented unless MSBs are adequately maintained on the same device.
- C. Host-based intrusion detection controls can be used in place of applying MSBs on the same device.
- D. They should both be implemented on all servers as part of a robust security architecture.

Answer: A

The correct answer is A. Both of these items are security controls that apply to devices on the network. While HIDS will be exposed without a good MSB in place (B), it is not a prerequisite. HIDS can in no way replace MSBs on a device (C), one looks for attacks by reviewing the logs, the other is a set of configuration controls, which

may enable attacks that a HIDS signature would see as normal and acceptable in most cases. The implementation of both (D) would be recommended only in situations where the risks were significant enough to warrant such an action and certainly not on all servers on the network.

92. During a network security review, the IS auditor determines that the firewall rule set is incorrectly built to protect the organization from the risks that are unacceptable to the business. The IS auditor should

- A. Immediately notify the IS organization management so corrections can be made to prevent further vulnerability.
- B. Discuss the issue with audit management and prepare the findings and recommendations for their report.
- C. Point out the deficiency to the firewall support staff, but note the state the controls were found in at the time of the review.
- D. Look at the rest of the controls to ensure that the risk has not been mitigated by some other method before doing anything.

Answer: D

The correct answer is D. Unless the firewall support staff is completely incompetent, there is probably a reason that the controls are set up the way they are, given the risks and environment that this staff manages day to day. Before alerting any management and possibly embarrassing yourself, you would be well advised to first check around for mitigating controls or the acceptance of risk. If that does not satisfy the control need, ask the support staff (C) to ensure they are aware of the situation. Conferring with audit management (B) would be the next step before approaching the IS management (A) and bringing up a potential situation (or possible embarrassment or confrontation) to their attention.

93. What is the primary purpose of a DMZ in a network architecture?

- A. To provide a place where authentication can occur before enabling access to sensitive data
- B. To separate business logic from classified data
- C. To provide a neutral zone where transaction requests can be made and honored without affecting the security of either adjacent zone
- D. To provide a location for proxy servers and drop off servers to reside without reducing the security of the more secure adjacent network zone

Answer: C

The correct answer is C. DMZs are intended to be a no mans land where neither side is trusted and exchanges or transactions can occur, similar to military DMZs. Business logic should not be housed in a DMZ, and classified data certainly should not be either (B). Authentication may occur in this region but that is not the primary purpose. DMZs do provide a location for proxies and other devices (D) but not to address security on only the more secure adjacent network. DMZs also provide a safe area for the lesser secure networks as well.

94. When evaluating the encryption used to protect a data transmission over the Internet, which of the following is not a relevant security control?

- A. Virtual private network
- B. Message digest
- C. Digital certificate technologies
- D. Secure sockets layer technologies

Answer: B

The correct answer is B. A message digest is a computation performed on a message that results in a one-way hash number. This one-way hash number is used to indicate the authenticity of the message received by comparing a reperformed digest computation on the same message to see if the same hash is the result. It is not an encryption-related control, but it is used to validate an encrypted message. The other three items are all encryption-related control techniques used for Internet-based transmission control.

95. Network intrusion detection and incident response are important parts of any security program. What aspects of an audit review must be included when evaluating these programs?

- I. Proper staff levels and training of the staff to react and respond to issues as they present themselves
- II. Establishment of a need for using either of these techniques based on the possibility of them actually being required
- III. The response time requirements and the ability of the program in place to meet those needs
- IV. Managements commitment to the programs and their support for enabling them to function when necessary

- A. I, II, III, and IV
- B. I, II, and IV only

- C. II, III, and IV only
- D. I, III, and IV only

Answer: D

The correct answer is D. All of the items listed are important aspects of both network-based intrusion detection systems and an incident response program, except for considering whether there is a possibility of their need or not. Even if the network is completely off-line from other connectivity points, which is unlikely, there will always be a need for an incident response process because security is not foolproof and incidents will always occur at some level. NIDS may be required to a lesser extent, but network-connected systems are attacked continuously from Internet sites and to not use NIDS by choosing to accept the risk would be a rare situation.

96. While evaluating third-party connections in an organization an IS auditor discovers PCAnywhere software resident on a financial workers desktop workstation. Which of the following controls would be seen as the strongest risk mitigate to unauthorized network access in this situation?

- A. The software is used only for the remote control of the workstation and access must be authenticated by dial up server controls first.
- B. The software may be correctly configured to use network authentication prior to enabling connection through a modem to it.
- C. The modem is unplugged and only connected when needed.
- D. The software is configured to use dial back and only enables outgoing connections made to known numbers.

Answer: A

The correct answer is A. The strongest control is to only allow the software to enable access to the device from a previously authenticated session from a trusted authentication device on the network. The other controls are configurable by the users and no assurance can be made that these settings will not change over time and in changing circumstances. Without a modem connected to the workstation, no outside connection to the network can be gained.

97. In an evaluation of virus protection processes, which three controls cover the most risk of those listed here?

- A. Virus protection deployed on every workstation, the blocking of dangerous attachments in all email at the mail servers, and a

- strong user education program about email viruses
- B. Virus protection active on all mail servers, the blocking of dangerous attachments in all email at the mail servers, and a strong user education program about email viruses
- C. A strong user education program about email viruses and virus protection that is actively enforced on all workstations and the blocking of dangerous attachments in all emails at the mail servers
- D. Virus protection on all mail servers, the blocking of dangerous attachments in all emails at the mail servers, and virus protection that is actively enforced on all workstations.

Answer: D

The correct answer is D. The combination of active protection on both the mail servers and workstations, in addition to blocking suspect attachments provides the strongest defense. User awareness (B) and (C) is a good control to have in place but will not be as reliable as up-to-date software controls that are managed centrally. Response (A) only indicates virus protection deployed at the workstation, but it is not necessarily forced to remain on at all times. These controls are often defeated by users when they are given the chance or when the controls are not kept up-to-date, making (D) a better answer.

98. Which of the following is not a control to address the risks associated with social engineering attempts?

- A. Asking for a name of a person to call back, documenting all of the requests, and validating the person by some means before granting access
- B. Adding the physical security responsibilities to the systems support people because they know who needs access to the operations center best
- C. Following the rules for access and permissions at all times to avoid opportunities for allowing your guard to be down
- D. Developing a healthy suspicion and learn to think like an attacker

Answer: B

The correct answer is B. Adding the physical security responsibilities to the systems support personnel may seem logical, but it will result in segregation of duties problems and lead to unclear primary responsibilities when conflicts arise. These responsibilities

also may require the support person to be in two places at one time, leading to the abandonment of one or the other, usually the add-on responsibility. The other controls are all good social engineering controls.

99. What is the most important control concern associated with the logging and monitoring of system or network activity?

- A. Ensuring that the information is time synchronized so forensic analysis can be accurately performed
- B. The placement of the sensors and protection of the logs from the systems administrators access
- C. Developing exception-based reporting and log correlation processes to reduce the amount of log review required
- D. Having the staff support available to read through the logs and take action on the results found

Answer: D

The correct answer is D. All of these factors are very important to the implementation of a successful logging and monitoring process, but the most important is being able to read the results and react to the information found. If issues are not identified and actions are not taken, the rest will not help control security.

100. When evaluating personnel safety controls in an IS operation, what is the best method to use for evaluating its sufficiency?

- A. Obtaining copies of the safety and emergency evacuation manual to evidence compliance with the requirement for procedures and documentation
- B. Reviewing the records of testing of personal safety devices and their maintenance histories
- C. Spot interviewing a few passing IS staff personnel and asking them about their knowledge of the safety measures and procedures
- D. Looking for posted evacuation signs and personal safety equipment stored in easily accessible locations to the users

Answer: C

The correct answer is C. The best way to determine if the staff on-site at an IS organizations facility has been adequately trained and personal safety has been planned for in the area is to ask someone who should know what the response should be when emergencies arise. These circumstances are immediate and cannot wait while the manual is located and the procedure is looked up. Staff should know at least

the basics of what is required to be taught to them on a routine basis.

101. What is the most challenging aspect of evaluating physical security controls in an IS organization?

- A. Assessing all of the numerous controls and ensuring that each one is managed properly
- B. Determining how to assess flexible situations such as security movement and the belongings of VIPs and visitors
- C. Being able to obtain proof of the physical security controls effectiveness in preventing or deterring unauthorized acts
- D. Touring the physical site and inspecting the controls to ensure that they are functioning properly

Answer: C

The correct answer is C. The most difficult part of drawing a conclusion when it comes to physical security is determining whether the controls are effective or not. It is easy to tell when a physical control fails because a breach occurs. But unless partial damage occurs when access is attempted, there will be little evidence that the controls are sufficient or not robust enough. This opinion will be a judgment call drawn from the IS auditors professional opinion.

102. In a review of environmental controls, all of the following are factors that need to be considered except

- A. The need for power continuity and the deployment of UPS, batteries, and generators as applicable
- B. The maintenance and testing schedule recorded for the fire suppression systems that protect the information systems
- C. Personnel evacuation plans and emergency exit routes posted in the operations center
- D. Moisture and temperature monitoring and tracking over time

Answer: C

The correct answer is C. Personnel evacuation is not an environmental control concern. If the controls function properly, personnel evacuation will not be necessary. You should ensure that the audit scope adequately defines the boundaries of the audit review in areas like this before proceeding with the engagement.

103. An IS auditor is reviewing an organizations contingency planning and recoverability. What is the most important factor to consider for the success of the recovery plan?

- A. The plan has identified all of the critical applications required to be covered for the business to survive.
- B. The plan is stored off-site.
- C. The process is supported by senior management and funded adequately.
- D. Back ups are made and moved off-site regularly.

Answer: C

The correct answer is C. The most important factor to consider for the success of a recovery process is the commitment and funding of the solution by management. Without proper support, successful recovery will not be a priority of the organization and funding and resource commitment will not be sufficient to achieve the goals. The other items listed here are necessary attributes of a recovery process, but the support of the leadership is paramount to all other factors.

104. When reviewing business impacts of possible disruption scenarios, which of the following criteria should be considered?

- I. The likelihood customers will take their business somewhere else and not return
 - II. The potential losses in terms of buildings and equipment
 - III. The costs associated with redeploying a process to replace the one that is lost
 - IV. The time it would take to fully recover and return to processing
 - V. The losses of current business from not meeting existing commitments
- A. I, II, and III only
 - B. I, II, III, IV, and V
 - C. I, II, III, and V only
 - D. II, III, IV, and V only

Answer: B

The correct answer is B. All of these factors should be considered in a Business Impact Analysis (BIA). Each factor contributes to the decision-making process of how severe a loss might be experienced and what the tolerance may be for loss, if in fact, there are many other factors to consider as well. Even the time it would take to recover (IV) is a factor, because when processing and service cannot be provided, the associated revenue potential cannot be realized. The longer this situation continues, the more loss can be inferred. This also will compound the likelihood that customers will have to turn to other sources for satisfying their needs.

105. An IS auditor determines that external consulting was used to create a recovery plan. Which of the following actions would be most appropriate for the IS auditor to take?

- A. Review the costs and contract deliverables for the consulting engagement and assess the adequacy of the contract.
- B. Review the methodology used by the firm and assess its appropriateness for the engaged organization.
- C. Ensure that the decisions made by the consultant seemed reasonable for the given business and organizational structure.
- D. Review the resultant plan and ensure that the business and IS staff were involved in inputting to the final product.

Answer: D

The correct answer is D. The most appropriate action to take is to ensure the organizations business and systems people were involved in building the plan. Recovery plans are unique to the organizations that they represent and cannot be dictated beyond format and approach. The contract and deliverables may be interesting (A) and the methodology should be at least relevant (B). If the consultant is making decisions for the business (C), this would constitute a material weakness because they could not possibly know as much about the business and their needs as those who run the business daily.

106. When reviewing a business and systems recovery plan, which of the following will be most important to find within the contents of the plan?

- A. Simple checklists depicting the steps that need to be taken to affect a recovery
- B. Change control information related to what has changed since the last plan update
- C. Call trees depicting the recovery teams and their contact information
- D. Inventories of hardware and equipment used on-site

Answer: A

The correct answer is A. The single most important element of a recovery plan is the steps needed to affect the recovery. Without these steps, there is no plan to carry out. The other items have relevance in support of the recovery procedure but are not as important as the procedure itself.

107. When reviewing the rationale for recovery options and decisions, which of the following best describes the correct approach for determining the appropriate direction for recovery planning?

- A. Planning for a recovery scenario that will not be costly to implement a solution for while still meeting the requirement for a recovery plan
- B. Looking at all options for the worst case disaster scenario and picking the solution that is cheapest while still meeting the needs of the business
- C. Determining the downtime associated with each recovery option and deciding on the one that will recover the business most quickly
- D. Determining the most likely disaster situation and picking the solution that most closely represents the existing processing configuration

Answer: B

The correct answer is B. Obviously, planning for the easy way out and only performing a recovery planning cycle to meet the requirement (A) will not result in a satisfactory recovery process for most businesses. Downtime (C) is not the only consideration when determining recovery strategies, and overall loss reduction should be the paramount determining factor. Even though picking the most likely disaster scenario is the right way to proceed, the existing processing configuration should not matter compared with the ability to recreate the user experience (D). The overall cheapest solution, considering all costs both related to out of pocket and related to downtime and customer impact while still meeting the business need, will be the best answer.

108. A business continuity plan should address the recovery of

- A. All mission critical computer applications
- B. Only those applications related to generating revenue for the business
- C. All applications needing recovery within the first 24 hours after a disruption
- D. Applications and processes determined by management to be high priority to management

Answer: D

The correct answer is D. Similar to the security discussions, management

has to make the decisions for what needs to be recovered so that the business they are accountable for survives. Business and operations management must educate them and provide them with the expertise to make risk-based decisions that will in the end be their responsibility. They alone must determine whether mission critical should be included on the list (A) or how relevant revenue generation is to the survivability of the business (B). Certainly the first 24 hours will be critical (C), but it is not the only criteria either.

109. Which of the following application attributes are not relevant when determining the priority order for recovery?

- A. The dependency of the critical applications on the output of this particular application
- B. The need for critical applications to be recovered in order to supply input to this application
- C. The importance of this application to the business processing needs
- D. How much downtime is acceptable to the users of this the application

Answer: B

The correct answer is B. Whether critical applications feed this application or not has little bearing on the recovery priority of the application. The dependency of critical applications on the one being examined will affect its relative priority, however (A). The particular applications downtime tolerance (D) and its importance to the business users (C) also will be relevant factors for determining priority.

110. To be effective for disaster recovery, back up copies of computer information should be

- A. Stored on-site in the production environment in a fireproof and watertight container
- B. A series of incremental back ups labeled and stored properly in the media library
- C. Moved off-site as quickly as possible
- D. Labeled and cataloged, corresponding to the recovery plans and sent to the location specified in the plan

Answer: D

The correct answer is D. While it is important to move back ups off site quickly (C), without the related documentation, media location identification, and recovery steps mentioned in the correct answer,

the recovery would not be effective. Answers A and B are incorrect because the media should not be kept on-site, even if it is labeled properly and stored in fireproof containers.

111. When evaluating recovery plan documentation, an IS auditor determines that the plans execution will result in the exposure of sensitive data to team members that do not have a need to know for this data. The auditor should

- A. Notify management of a material weakness in their final audit report.
- B. Recommend that stronger controls be applied to the data management during the recovery process.
- C. Focus their efforts on the recoverability of the business processes and note the control weakness for follow-up after the recovery is complete.
- D. Review the procedures for compensating controls or manual processes to control access during recovery.

Answer: C

The correct answer is C. Recovery plan documentation should be reviewed for its capability to provide for an effective recovery of the business process, not for its ability to protect the data with production level controls during the recovery efforts. This will not be a reportable finding (A) and stronger controls would not be an appropriate recommendation ,in this case (B) for the most part. Compensating controls may be relevant (D) and give the IS auditor some assurance, but this is not the purpose for evaluating recovery documentation.

112. Incorporating systems and process changes into a recovery plan is an important part of keeping it relevant and viable for the recovery of the business process. Which of the following approaches would best meet the needs of the business for ensuring that the changes are appropriately incorporated into the recovery plan documentation?

- A. Testing the plan and making changes only as necessary to support the recovery plan process requirements
- B. Sending all IS operational changes to the recovery site for inclusion into the recovery documentation
- C. Updating the documentation during the periodic review of the plan and incorporating only the relevant changes
- D. Making the business unit recovery teams accountable for their respective portions of the recovery plans and related updates

Answer: A

The correct answer is A. Testing the plan is always the best way to ensure that it works and any corrections or changes needed are appropriately addressed. All changes may not be relevant to the plan or its procedures (B) because a full IS system replacement may not be the scope of the recovery process. Updating only during a periodic review (C) may not meet the business needs, especially if major process changes are not updated to the recovery plan documentation in a timely manner. Many teams inputting into a plan (D) will eventually result in unsynchronized changes and processes that will not match up when necessary for recovery purposes.

113. When reviewing a systems disaster recovery plan, an IS auditor should look for operations procedures that

- A. Have been approved by senior management
- B. Follow the procedures used by the IS organization in normal production
- C. Describe how to perform the successful operation of the recovered subset of operations
- D. Describe all aspects of the current process in detail

Answer: C

The correct answer is C. Disaster recovery is a stressful situation and the procedures to recover a system should be kept as simple as possible. Describing all current processes in detail (D) may not be relevant to the recovery process and will interfere with getting the job done, in some cases. The procedures used in normal production (B) also may not be relevant as recovery is often the bare minimum necessary to survive. You should not expect to see operational procedures approved by management; they would not understand what they were approving. Only the procedures needed to recover the subset intended to be recovered should be found as procedures in the recovery manual.

114. The declaration of a disaster that invokes a recovery plan process should be

- A. Made by the IS organizational manager as soon as the need is identified
- B. Documented as a process requiring formal approval and an audit trail to provide evidence of the decision
- C. Only done after a repair and restore has been tried and has failed
- D. A decision of the business senior management after considering

all alternatives, risks, and costs

Answer: D

The correct answer is D. The IS organization should not take it upon themselves to declare a disaster (A) because of the impact to the overall business and disruption a recovery process will make to the business as well as the IS operations. Some repair and restoration may be initiated first (C), but this will depend on the nature of the disruption and damage experienced and is not necessarily the best first step in all cases. Times of emergency are not when audit evidence and formal procedures are called for in a business setting (B), they are a time for decisive action and insistence on approval and evidence is often inappropriate. Senior management should make the decision for the entire affected organization only after considering all of the available alternatives and weighing the cost and benefit of each of them to the long-term survivability of the organization.

115. When reviewing the information recovery procedures, an IS auditor would be least concerned with finding procedures that

- A. Lay down the last complete back up and then all of the subsequent incremental back ups that are available
- B. Recover all available information from the available back up tapes and move forward with the available information
- C. Use hard copy transaction records to return the transactions processing history to the time of disaster from the last available back up
- D. Use the best information available and reconcile the inventories to understand the transactions that may have been lost during the disaster or disruption

Answer: B

The correct answer is B. A procedure that recognizes that some electronic records are bound to be lost and that requires hard copy transaction information be created and used to recover to the point of failure of the systems is the next best recovery model for a transaction processing system. The best would be mirrored, journaling at an off-site location. The other answers described here do not recognize the transactions in progress since the last back up was taken and will be less effective in providing for a complete recovery.

116. The most important aspect of a recovery plan in the initial hours of a recovery process will be that

- A. Call lists and rosters are included for contacting the recovery teams
- B. People have been trained what to do and where to meet to gather and begin recovery without the documented plan
- C. A disaster is declared by management and the EOC is activated as a control center
- D. Testing results have been included to show current recoverability

Answer: B

The correct answer is B. Knowing what to do without any of the plan documentation is critically important in the first hours of the recovery process when manuals and procedures may not be available from staging and storage areas. Call lists and rosters are critically important to this effort but will not be useable from within the recovery plan stored with the recovery materials or destroyed by the disaster (A). These lists and rosters must be available immediately; the copies with the recovery plan will only be used if all else fails (or as a check to ensure that everything was covered by the interim processes, which were used immediately after the disruption occurred). The other two items (C) and (D) are nice to have but are not as important as the training of key individuals who will lead the initial recovery of gathering and assessment processes.

117. When reviewing a recovery plan, an IS auditor will be least concerned with plans for managing the press and media by

- A. Providing a location away from the immediate action where the media and press can be briefed periodically by the designated spokesperson, and allowed the opportunity to ask questions
- B. Providing space for the press and media inside the Emergency Operations Center (EOC) with immediate access to recovery teams
- C. Using a policy to tell the media and press as little as possible and denying all rumors with a "No comment" reply
- D. Using a policy that encourages the media to talk to the workers and ask questions as they come in and out of the recovery area as a way to communicate without interfering with management and the recovery process

Answer: A

The correct answer is A. The best way to deal with the media is to acknowledge their need for information and provide it in a forthright and controlled manner by a person who can provide an authoritative and consistent message that management can control.

Direct access to the EOC (B) of the recovery workers (D) may result in reputation damage by unanswered questions as work in progress could provide opportunities for wrong conclusions and unchecked tempers to put the organization in a bad light. Denying access to any information (C) leaves the media to draw their own conclusions, which may not be complimentary to the organization.

118. What is the primary advantage of a hot site over a cold site for recovery planning?

- A. There is less work to do at the time of disaster because the site management will prepare it for you.
- B. Communications have already been tested, thus providing for a higher probability of success.
- C. Testing has occurred at this location in the past, so recovery teams are more familiar with the facilities and how to go about affecting a recovery.
- D. Downtime is minimized because equipment does not have to be configured and installed.

Answer: D

The correct answer is D. The primary benefit is the reduced downtime. Costs are generally higher and this trade off here is time for money. If recovery time is critical enough (and this needs to be justified and documented), then the costs will be acceptable compared with the losses that may occur. The other items listed are all benefits of the hot-site recovery plan, but downtime reduction is paramount.

119. When reviewing the plans for business operation recovery, an IS auditor would be most concerned to find which of the following unaddressed by the plan?

- A. That there is adequate space for accommodating the business staff in an alternate site
- B. That computer workstations are available with the latest technology on them with which to perform the business processes
- C. That a desktop appropriate for the processing of the recovered business can be made available
- D. That connectivity to the EOC is provided for the business desktops for communication

Answer: C

The correct answer is C. Not having the right desktop configuration to perform the necessary business functions will be the most egregious

error when planning for business recovery. Adequate space for the business staff may not be necessary (A), depending on the recovery plan and an analysis of what functions are critical and need to be manned for recovery processing. The latest technology (B) is certainly not a requirement for success. Connectivity may be very important to the operational processes (D) but not necessarily to the EOC this is commanding the recovery effort and not the IS operations.

120. When observing the testing of recovery in a dual-site, operational recovery plan configurations, what should an IS auditor expect to see?

- A. Business continues as it normally would with no downtime or disruption
- B. Additional equipment being quickly turned on and added to the configuration at the surviving site to accommodate full processing with minimal disruption
- C. Two identical sets of processing equipment set up for hot fail over from one site to the other with no impact on the users
- D. A procedure that sheds some testing, reporting, and lesser essential functions allowing for the concentration of the surviving site on the critical business processing to be performed

Answer: D

The correct answer is D. A dual-site, contingency arrangement is one where a single (sufficiently large) operation splits its processing between two sites, spreading its critical processing across both sites so a single failure will not completely disrupt any one of them. The balance of the sites processing, the lesser critical systems, and spread across the sites provides for the shedding of noncritical operations in support of the critical one if necessary.

121. When reviewing the recovery testing reports to management, an IS auditor will be most concerned if the following is not part of the report:

- A. An assessment of the time it takes to recover compared to the management expectations for recovery and a gap analysis of the potential impact that any shortfall may have on managements risk or loss expectations
- B. A comprehensive list of all of the problems and the resultant assigned action items
- C. A description of the process used to test the recovery, depicting the assumptions made about the recovery situation that was

being tested

D. A list of planned goals or milestones with an analysis of the ones that were achieved and those that were not successfully tested

Answer: A

The correct answer is A. The single most important part of communicating with management about disaster recovery testing is to report against the capability to recovery and the adjustment of expectations that management has, by which they make risk-based decisions on a daily basis. Without feedback on the risks and ability to control them through recovery for disaster, management will be unable to provide the correct guidance and direction to lead the company forward in a risk-managed manner. Expectations must be managed and funding and risk tolerance adjustments made through this reporting feedback mechanism. The other items listed may or may not be of interest to management, deepening their appetites for detail related to the progress being made.

122. When reviewing a systems development project, what would the most important objective be for an IS auditor?

A. Ensuring that the data security controls are adequate to protect the data.

B. Ensuring that the standards and regulatory commitments are met.

C. Ensuring that the business requirements are satisfied by the project.

D. Ensuring that the quality controls and development methodologies are adhered to.

Answer: C

The correct answer is C. The most important review objective for any assessment of systems development will be to ensure that the needs of the business are met as the result of the development. This actually incorporates the other objectives at a high level. You will not be able to satisfy the business needs without also addressing the security (A), standards and regulatory requirements (B), and quality objectives (D) as well.

123. When participating in an application development project, which of the following would not be appropriate activities for an IS auditor?

A. Testing the performance and behavior of the system controls to

ensure that they are working properly

B. Attending design and development meetings to monitor progress and provide input on control design options

C. Reviewing reports of progress to management and contributing to their content based on fieldwork and opinions forms from reviewing documentation provided

D. Assisting in the development of controls for application modules and user interfaces

Answer: D

The correct answer is D. It is a violation of duty segregation for an IS auditor to design and develop systems or controls that they will have to subsequently audit and provide opinions on. Independence and objectiveness are no longer preserved in this case. Testing of controls (A) is an objective and independent function and would be an appropriate contribution to the process. Providing input on control design decisions (B) also would be acceptable as long as the decisions were made by the project team and not by the auditor. Providing input to the reports related to the projects progress and performance (C) also is acceptable as long as the auditor does this in an objective and independent manner.

124. When reviewing an application development project that uses a prototyping development methodology, with which of the following would the IS auditor be most concerned?

A. The users are testing the systems before the designs are completely documented.

B. The functional requirements were not documented and agreed to before the prototyping processes began.

C. The documentation of the coding processes and testing criteria were not complete and well referenced.

D. The systems specifications were not signed off on before the development processes were started.

Answer: B

The correct answer is B. It would be most important in the prototyping development scenario for the business users and management to agree on what the requirements and outcomes are before starting to evaluate the prototypes of new systems. Otherwise, the business problems are not fully known and the solutions presented have little chance of meeting the undocumented need. User testing of designs (A) is a natural part of this process type. Overlap of the functional specification process, the system design process, and the development

cycle (C) also is an expected behavior of prototyping methodologies. Strict sign off of the project movement from one phase to another (D) would not be expected in this process as a result.

125. In a systems development life cycle, the following process steps occur:

- I. Systems Design
- II. Feasibility Analysis
- III. Systems Testing and Acceptance
- IV. Systems Specification Documentation
- V. Functional Requirements Definition
- VI. Systems Development

What is the natural order of the processes in an SDLC methodology?

- A. V, IV, II, I, VI, III
- B. V, II, IV, I, VI, III
- C. II, IV, V, VI, I, III
- D. II, V, I, VI, III, IV

Answer: A

The correct answer is A. Classic Systems Development Life Cycle (SDLC) methodologies begin by understanding the business or functional requirements and then a feasibility analysis is performed on the solution options. Systems specifications then are further defined based on the accepted solution and approach from which a design is created. That design is developed into an application and that application is tested and finally accepted by the business.

126. Where would be the ideal place for an IS auditor to find the first consideration of security controls?

- A. During the design phase of the system development process
- B. When determining what the systems specification will need to be
- C. When reviewing the functional requirements for the system
- D. When testing the system for overall compliance to regulatory, privacy, and security requirements

Answer: C

The correct answer is C. Security should be considered as one of the functional requirements as early in the process as possible. Studies have shown that the security controls are seven times more costly when applied to a system that is already developed as compared to one with security designed into a system as one of its functional

requirements. The later in the process that the first consideration of security is identified, the higher the risk is that the security requirements will not easily fit into the process that has been envisioned up to that point.

127. The main difference between a functional requirement and a systems specification is

- A. A functional requirement is a business process need, and a systems specification defines what the system must do to meet that need.
- B. Functional requirements address the details of the need from a data perspective, and systems specifications define them from an operational systems perspective.
- C. Functional requirements define more of what needs to happen, and systems specifications define how something will happen.
- D. Functional requirements define all aspects of the process flow from a business process perspective while systems specifications are more hardware and operating system-specific.

Answer: A

The correct answer is A. The most important difference between functional requirements and the systems specification are the business perspective and the solution requirements or system needs perspective. Both sets of information and related documentation require a data and operational view (B), and both are a combination of what and how needs and their solutions might be addressed (C). While functional specifications are a more business driven perspective, systems specifications are not necessarily limited to hardware and operating system perspectives (D). They also need to address application logic-related processes and requirements.

128. Which of the following is not a criterion for an effective feasibility analysis report?

- A. An assessment of the proposed solution approach and its viability in the existing business process
- B. An assessment of the impact of the new application on the business processes and workflows
- C. An analysis of the costs and projected benefits of the application, determining overall benefit or detraction from the business prospects of the overall business strategy
- D. An assessment of the systems development methodology proposed for the design of the application

Answer: D

The correct answer is D. How the development process may be approached is not part of the feasibility analysis and may not be determined until after all of the requirements and constraints are gathered and analyzed. Assessments of proposed solutions and determining their viability (A) is the objective of the feasibility review. Impact assessments for proposed solutions (B) are part of the determination that must be made to go forward with the project. ROI and a cost/benefit analysis (C) also are important aspects of this assessment.

129. If there was a most important place for the quality assurance teams to be involved in the development project, where would that place be?

- A. During the testing and code migration from test environments to production-ready code
- B. At the beginning of the project to ensure that quality standards are established and understood by all of the development team members
- C. During the code development to ensure that processes are followed according to standards and are well documented
- D. In the final phases to ensure that all of the quality processes and requirements were met prior to signing off on final acceptance

Answer: B

The correct answer is B. Quality Assurance (QA) should be used as a compliance and checking function throughout the systems development process. However, the most important part of the QA process is the establishment of standards and teams education of these requirements. Many other roles are supported and enhanced by the QA function, and they are instrumental in objectively ensuring the processes will be supportable and built according to the organizations methods and conventions (C). They place a key role in checking and testing code migration (A) and ensure the usability of the final product (D). But without established parameters from which to measure efforts, quality cannot be assured.

130. What aspect of the systems development testing process needs to be addressed during the systems design process?

- A. The use cases are documented to show how the product is supposed to work when completed.

- B. The detailed work plans and process steps are defined so that they can be checked for completeness during testing of the development process.
- C. The expectations and outcomes of the development process are defined formally to be used for testing criteria.
- D. The project design is checked against the functional requirements.

Answer: C

The correct answer is C. Testing criteria are formulated from the expectations and intentions of the design and its documentation. In fact, test scenarios should be sketched out for the design parameters as part of the design process. This ensures that the design and its incorporation of the requirements and specifications will be honored as testing criteria after the development process is concluded. Work plan steps are not relevant to testing of the systems performance (B) and use cases are only examples (A) and may not be detailed enough to drive out specific testing and evaluation of application development points. The project design should ensure that the functional requirements are all addressed (D), but this does not drive testing criteria directly either.

131. When reviewing a systems design, an IS auditor would be least concerned to find that which of the following was not considered?

- A. The provisions for adequate internal controls and the addressing of regulatory requirements
- B. Increased costs and delays in the project deadlines
- C. The observance of quality assurance standards and processes
- D. The failure to consider environmental and facility needs as part of the design

Answer: B

The correct answer is B. Time delays and cost overruns may be indicative of project management control issues for the overall project. But when reviewing the design itself, these issues are of the least importance to an IS auditor. The design must have considered the internal control needs (A), the QA requirements (C), and the environmental (D) to adequately address the needs and result in an acceptable application.

132. When reviewing a systems development project, an IS auditor observes that the decision has been made to use a purchased vendor package to address the business requirements. The IS auditors should

- A. Discuss the contract and costs with the vendor to ensure that the best deal has been obtained for the organization
- B. Review the ROI assumptions and decide whether they are still valid
- C. Review the contract for a right to audit clause in the agreement
- D. Review the build versus buy recommendation and determine that the costs and benefits are fairly stated in the recommendations made

Answer: D

The correct answer is D. The correct approach for an IS auditor is to review the decision documentation and to ensure the conclusions made are supported by the problems risk and benefit analysis. This documentation should be completed for all major decision points in the project to show that the best interests of the business were addressed in the decision. Auditors have no place dealing with vendors directly in any authoritative capacity (A) and contract clauses giving the right to audit will probably not be relevant to a purchased software product vendor (C). ROI assumptions will need to be adjusted after the impact and total cost reassessed, but it is not the auditors place to make business determinations on validity, for example. It would be more appropriate for the auditor to question documentation found to be deficient, but he or she would not declare something as invalid.

133. The most important issue with change control during the development of large scale systems is

- A. Managing the versions of code in development to ensure that testing will result in a workable system
- B. Ensuring that testing and back out procedures have been provided for each change
- C. Ensuring that maintenance and disaster recovery procedures have been documented for each change promoted through the process
- D. Tracking which module has been tested with other modules to understand the development progress

Answer: A

The correct answer is A. Ensuring that version control for several concurrent module development efforts can be managed effectively is the most important role that change control plays in the development process from the ones listed in this question. Back out and testing procedures (B) as well as disaster recovery and maintenance

documentation (C) are very important aspects of change control in a production system, but they are not as relevant during the development process. The module tracking aspects of change control (D) are more related to the testing than the development phase.

134. When reviewing a development effort where third-party programming staff are used, the IS auditor would be most concerned with?

- A. Ensuring that they are qualified and knowledgeable about the tools and techniques being used
- B. Ensuring that the code is reviewed independently from the thirdparty staff and ensuring that the ownership rights are maintained within the organization
- C. Ensuring that background checks are made for individual thirdparty staff members to protect the organization from undesirable persons participating in the effort
- D. The impact to the cost and timeline estimates originally presented and approved by management

Answer: B

The correct answer is B. The most important risks of third-party participation can be addressed with a solid code review integrated as part of the development process and contractually maintaining ownership of the products produced. Qualified personnel also are criteria (A), but this risk that can be mitigated also can be the code review. Background checks are more important than ever (C), especially if these programmers will be in close proximity to the business processes and are relatively unsupervised, which is not always the case. Finally, cost and time aspects are important (D), but this is not as critical to the result and the quality of the code being turned out.

135. An independent quality assurance function should perform all of the following roles except

- A. Ensuring that the development methods and standards are adhered to throughout the process
- B. Ensuring that the testing assumptions and approved modules of developed code are aligned to give a final product that meets the design criteria
- C. Reviewing the code to ensure that proper documentation and practices were followed
- D. Correcting development deficiencies and resubmitting corrected code through the testing process

Answer: D

The correct answer is D. Independent quality assurance functions cannot modify any code without violating their independence and segregation of duties. The other functions listed are appropriate actions for an independent QA function to perform.

136. Which of the following are not considered communication controls?

- A. Network traffic monitoring and alert systems
- B. Encryption techniques to limit accessibility to traffic in transit
- C. Access control devices that limit network access
- D. Bandwidth management tools to shift data based on traffic volumes

Answer: C

The correct answer is C. Access controls are boundary controls even when they are applied to the network and communication layers boundary. The other controls work at the communication layer and are communication controls.

137. Review of documentation in a systems development review is very important for all of the following reasons except

- A. Training and maintenance efforts require that good documentation be made available for their processes to work effectively
- B. Allowing the IS auditor to review the process without actually having to perform code-level reviews of programming efforts
- C. Disaster recovery and support processes depend on the quality of the systems and user documentation
- D. User effectiveness and production processing depends on the users ability to read and understand the manuals and procedures associated with the application development process

Answer: B

The correct answer is B. Using the documentation as a crutch to avoid detailed review as an IS auditor is not an important use of the development training manuals and systems documentation. The other uses described in the choices given are all necessary and relevant reasons to expect good, accurate, and easily understandable user manuals, training documentation, maintenance manuals, and operational procedures.

138. In reviewing a vendor solution bidding process during a systems development review, an IS auditor would be most concerned to find

that

- A. A vendor solution had been chosen prior to documenting the vendor criteria.
- B. The chosen vendors cost was not the lowest of the providers of an acceptable solution.
- C. Some of the vendors received more information about the bid request than the others did.
- D. Some of the bidders on the vendor list were not capable of responding effectively to the bid based on their business model and the product being requested.

Answer: A

The correct answer is A. All of these situations are cause for concerns over the bidding process from an IS auditors perspective, but the most egregious violation of best practice is to have chosen a vendor solution before the problems were formally defined and documented. The other items listed also should be investigated for mitigating controls or valid explanations, but without a problem definition the solution is driving the problem and not the other way around.

139. Which of the following is not a risk associated with the decision to use a vendor software solution?

- A. The risk that the vendor might discontinue support of a product that is mission critical to the business
- B. The risk that the costs and contract provisions might adversely impact the business model in the long term
- C. The risk that in-house support expertise might be insufficient to adequately address ongoing support and maintenances need of the product
- D. The risk that business needs for enhancements and corrections might not be addressed in a timely manner

Answer: C

The correct answer is C. In-house expertise needs for support and maintenance are greatly reduced by the use of a vendor package solution compared to developed applications, making this answer a risk that is not associated with vendor solutions. The other answers are all considerations of risk that need to be assessed if vendor solutions are being considered.

140. During go-live, security and change management controls are often

relaxed to facilitate the implementation. What actions are most appropriate for the IS auditor during this process?

- A. Raising concerns about the control deficiencies to business management and suggesting additional controls
- B. Waiting until the implementation process is completed and running audit and analysis tools on all transactions during the implementation period
- C. Recommending that the risks of reduced controls be accepted and encouraging the process to move into a more controlled phase as quickly as possible
- D. Observing the implementation process to understand the extent of control risk that is residual to the process and recommending prudent, additional steps to regain assurance of data integrity

Answer: D

The correct answer is D. The best course of action is to observe from a distance and determine the best course of action to mitigate any residual risk exposure from the implementation process. Raising concerns to management (A) will not be seen as value added and may impede progress on the project because some amount of risk must be assumed. Coming in after the fact to analyze for errors (B) will assume a higher risk level than may have actually been the case, resulting in more work than necessary. Accepting the risk and moving forward without assessing the exposure (C) would not be in the best interests of the business owners where the auditors objectives are to minimize risks and ensure effective application of the controls.

141. During the user testing of the application under development, the IS auditor would be most concerned if he or she found that

- A. Users were accessing the test system from their normal workstations to test the system
- B. Production data was being used for testing the system
- C. Users were not all trained to the same level of competency for the testing process
- D. Interfaces were simulated to provide input to testing and were not actually being represented by live input feeds.

Answer: B

The correct answer is B. Use of production data for testing purposes may provide real-world examples of data to test with, but it will violate the security and confidentiality of the production data. Even if the data stewards give permission for the use of the data in a testing scenario, client data cannot be exposed to testing without additional controls to ensure that it has not been violated. This can be done effectively in a closed development and testing environment, but

that level of controls is not normal for development efforts. The other issues stated here also are of concern to the IS auditor, but the risks and materiality of each case will need to be assessed in order to determine the appropriate level of concern.

142. Corporate governance can best be described as

- A. A formal process of implementing controls across the system
- B. A process that ensures that all risks have controls associated with them
- C. The guiding principles and policies of the organization
- D. The process for ensuring that all risks and accountabilities are managed within a business

Answer: D

The correct answer is D. Corporate governance can best be described in terms of responsibility and accountability for governing the actions and behavior of the corporation. Implementing controls (A) is only part of the business management process implied by corporate governance. Corporate governance may provide risk and control management (B), but that also is only part of the answer. Guiding principles and overall policy also is part of the overall management of risk and accountability process implied by corporate governance, but ensuring that all of these things are managed well best describes what corporate governance is all about.

143. When reviewing a corporate governance system, an IS auditor would be most concerned to find which of the following deficiencies in the process?

- A. Gaps in the handing down of the authority necessary to carry out the responsibilities given to unit management
- B. Lack of an enforcement and disciplinary process for ensuring that governance and direction is in effect
- C. Unit level goals that do not tie directly to the overall mission of the business
- D. Incomplete measurement processes for ensuring that the governance direction is carried out

Answer: B

The correct answer is B. All of these items are weaknesses in the corporate governance system. Gaps in the authority to perform against the responsibilities are an all too common problem in business (A). Unit level goals should tie back to the overall goals in some way (C)

and measurement processes should completely and accurately show senior management how well the governance direction is being carried out in the business units (D). However, the most significant item of those discussed here is the lack of an enforcement process and means to ensure that the direction is performed against along with sanctions and disciplinary controls to make ensure these things get done. Without this process, there is no penalty for nonperformance and the intent of the governance process must be suspect.

144. What is the most important thing to keep in mind when reviewing a business process for best practice design?

- A. The state of the art solutions that are available in the market to perform these business functions
- B. The current business model and its overall performance metrics
- C. The requirements, business goals, and core competencies defined by the business model
- D. What the competition is doing

Answer: C

The correct answer is C. The most important aspect to keep in mind when reviewing a business against the state of the art practices is the goals and mission of the business. This should be the prime driver against which change and improvement are to be measured. Knowing what best practices are out in the marketplace (A) will be input to the process, as well the current performance measures (B) and the intelligence about the competition (D). However, the goals of the business should be the driver against which success is measured.

145. What is the primary role that Key Performance Indicators (KPIs) have in supporting the business process effectiveness?

- A. KPIs show when controls may not be working properly.
- B. KPIs are used to show that the service levels and business requirements are being met.
- C. KPIs show the percentage of a systems uptime and measure the output volumes and speeds.
- D. KPIs can be used to draw conclusions about the overall performance of the processes and target variances for follow-up analysis.

Answer: D

The correct answer is D. KPIs can be used to show many detailed

and summary reportable facts and figures, and are also excellent controls in and of themselves for giving management a warning system when the systems and processes are not performing up to their expectations. The primary role of KPIs as it relates to business effectiveness is the big picture view or overall performance conclusions that can be drawn from their review. The other items listed here are all subset information indicators to that overall, primary function.

146. Management controls are intended to do all of the following except

- A. Enable for individual units to establish policies to meet their particular needs.
- B. Provide baseline guidance and direction for the entire business culture and style.
- C. Set rules for the business processes that are followed by all units and departments.
- D. Establish a framework for corporate governance and compliance.

Answer: A

The correct answer is A. Management controls are intended to establish overriding rules and principles that act as a baseline for guidance (B) and a corporate governance framework (D) for the entire business. These controls set down the rules for all units to follow (C) but do not usually provide for individual units to deviate or build their own set of policies.

147. When evaluating a business process reengineering project, an IS auditor would be least concerned to find that

- A. The staff that actually performs the current processes is not involved with the design of the redesign of the process
- B. Management commitment and support is not clearly stated in writing
- C. External facilitators are not involved in the analysis and streamlining of the existing processes
- D. The scope of the project has not been documented to include all of the existing facets of the business process being examined

Answer: C

The correct answer is C. All of the issues depicted here should be a concern to the review of a reengineering project. Managements commitment and support (B) would be the biggest concern if it were not apparent. Projects of this magnitude and impact cannot be successful

without the full support and funding by management.

Clearly a red flag should be seen if you find that the processing personnel, who know the current process and deliverables best (A), are not involved in the redesign. The other aspect of this concern would be the need to gain buy-in from those being impacted by the change in order for it to be accepted and succeed. If all of the interfacing aspects of the current process are not considered as part of the projects scope (D), there is definitely going to be some problems, or at a minimum some missed opportunities to capitalize on optimization and efficiencies. The least concern would be the involvement of external facilitators to tease out issues and opportunities that may be overlooked by those who work with the process daily. While the involvement of people unfamiliar with the current process provides opportunities to ask seemingly dumb questions, a rigorous discipline to examine all processes closely can provide this level of analysis as well, making this a less important issue.

148. All of the following are valid ways of measuring customer satisfaction except

- A. Sending out questionnaires with the product and asking for feedback on service and performance
- B. Using internally generated KPIs to see whether the performance levels are being met or exceeded
- C. Measuring repeat business and customer base growth from internal sales and shipping information
- D. Measuring the percentage of overall market share this particular business has in the market and its relative growth over time

Answer: B

The correct answer is B. Internally generated information, especially that which is not independently verified, is least acceptable as a measurement of external customer satisfaction. Questionnaires seeking direct feedback from the customers (A) and external information about overall market share (D) are independent measurements that show validated evidence of performance against customer expectations. Sales growth and shipping information also can be used to get a sense of this issue (B), but it should be gauged in comparison to the competition and the total market available in order to get the most accurate picture of the actual performance against the potential.

149. Which of the following are valid reasons for considering an e-business solution in support of the business process?

- I. The customer base is widely scattered and remote to the physical business location.
 - II. The costs of doing business over the Web have been shown to be more efficient for the business than other mechanisms.
 - III. Everybody is doing it.
 - IV. The sales department believes that adding functionality to the Web presence will move customers from a browse to a buy online model by making this business option available to them.
 - V. Real time and immediate support of the business transactions can be best supported by an online transaction model.
- A. I, II, and III only
 - B. I, II, III, and IV only
 - C. I and II only
 - D. I, II, and V only

Answer: A

The correct answer is A. Items I, II, and III are all valid reasons for considering an online solution for business processing. When customer locations are remote and disperse (I), online solutions add value to these existing customers and provide them options, making this a valid consideration. Anytime there is proof of lowered costs (II) supported by evidence, the consideration is a valid one. You may think that just because everybody is doing it (III) may be the wrong reason, but business trends go that way at times and consideration needs to be made or the business may get left behind. However, just because the sales department believes that if you build it, they will come (IV), the validity of the reasoning must be questioned by the auditor unless some substantiating evidence can be shown. Real-time, immediate needs are the worst rationale (V), because the use of the Internet cannot be assured and certain.

150. When reviewing the design and implementation of risk controls, it will be most important for the IS auditor to determine that

- A. All risks are being completely mitigated through the proper application of control mechanisms.
- B. Controls prevent risks situations from occurring wherever possible.
- C. As many risks as possible are addressed by the control that is being considered for implementation.
- D. There is a proper balance between the gravity of the risk and the control measure implemented.

Answer: D

The correct answer is D. Balance of the controls and the risks they are intended to manage is the most important aspect of a review of control implementation. All risks should not be mitigated completely (A) due to cost and overhead considerations. Preventive controls may be preferable in some instances (B) but certainly not right for all situations. While multiple uses from a single control may certainly simplify control management, it is not the most important aspect of the design and implementation process. Controls should always be applied commensurate with the risk of loss being faced by the residual risk that is being addressed by the implementation.

151. Preventive controls are primarily used to

- A. Stop a process and notify the operations that an error has occurred
- B. Keep an error situation from occurring by recognizing the condition and denying its occurrence
- C. Monitor and check error conditions that cannot be easily managed in other ways
- D. Address complex ranges of error conditions that can all be addressed by unique prevention condition statements

Answer: B

The correct answer is B. Preventive controls prevent a predefined error condition from being enabled to occur. Stopping the process (A) is not necessarily part of the way a preventive control may operate and the notification is more of a detective control behavior. Preventive controls must be monitored and checked periodically like any other control (C) making this a wrong answer. Preventive controls need to be defined for every unique situation they are intended to prevent, and they may be expensive and unjustified for complex ranges of error situations (D), which is why this is not the primary use of a preventive control.

152. When evaluating the effectiveness of detective controls that are applied to business systems, an IS auditor should consider the following:

- I. Whether preventive controls would be more appropriate for the risk type and possible loss scenario.
- II. The error rate and accuracy of the control in identifying out of bounds conditions.

- III. The reporting mechanism used to notify management of an error condition.
- IV. The cost of the control compared to the potential loss to the system.
- V. Whether the risk is significant enough to warrant any controls at all

- A. I, II, and IV only
- B. II, III, and IV only
- C. IV, V, and II only
- D. I, II, III, IV, and V

Answer: D

The correct answer is D. All of the items lists should be considered when evaluating detective controls. Risk and loss potential should be the primary drivers for determining how much control is needed. The way in which the control operates, its success and failure rates, and how it communicates results to management are all important considerations as well.

153. What is the primary difference between a corrective control and a detective control where business processes are concerned?

- A. Business processes cannot be corrected in midtransaction, thus making corrective controls less applicable.
- B. Best practices typically indicate preventive controls over either of these other two control choices.
- C. Corrective controls include detection as part of the way these controls operate and then fix the problem as well.
- D. Corrective controls can only fix a small range of errors, while detective controls can detect a far greater scope of possible error conditions.

Answer: C

The correct answer is C. Corrective controls correct the problem or error condition after detecting that it has occurred. Business processes are no different than information systems or other processes when it comes to control types used to mitigate risk.

154. What is the primary difference to keep in mind when evaluating automated and manual controls?

- A. Automated controls can operate in an unattended fashion, which requires less testing and monitoring.
- B. Manual controls require human interaction to be successfully deployed and must consider human fallibility as part of the

accuracy assessment.

C. Potential losses are more difficult to measure with manual controls because the error rates are more difficult to measure.

D. Training and documentation are required for manual controls while automated controls do not require such documentation.

Answer: B

The correct answer is B. The human factor is the most important consideration when evaluating manual controls against automated controls. Training and documentation (D) is one aspect of this human interaction as a control mechanism, but there are other aspects, such as human nature, which also play a part in this analysis. Potential loss when using manual controls (C) may be a factor to consider in this evaluation, but it is not the primary concern. Although the automated controls are automatic by design, they still must be monitored and tested (A) commensurate with the risk they are put in place to control.

155. A risk assessment has determined that the losses that could be potentially incurred with the delivery system of a business may cost up to \$10,000 per month. Preventive controls have been recommended that will save the company \$7,000 per month but this control will take three months to implement at a cost of \$100,000 and at an ongoing cost of \$1,000 per month. The business process has a life span of five years and has been in production for one year. Is the control justified?

A. Yes, the savings over the remaining life of the process would be \$315,000, thus justifying the expense.

B. No, the \$3,000 per month that will be missed over the life of the process (\$144,000) exceeds the cost of the control.

C. Yes, the total cost of the control over the remaining process life is \$145,000, while the potential loss without the control would be \$480,000.

D. Maybe, if the potential savings over the remaining life of the process (\$315,000) minus the total cost of the control (\$145,000) represents a material risk to the company's management (\$170,000), management may consider implementing the control and avoiding the risk.

Answer: D

The correct answer is D. This question is about potential loss not actual loss. The risk of loss is a management decision that must be

weighed against the probability of occurrence (not referenced in the problem), and the appetite for risk by management. The cost of funds and other priorities may influence this decision as well. While control looks justifiable on paper (savings exceed cost over the life of the process by a significant amount), the probability of that loss occurring to the business needs to be factored into the decision process.

156. The Annual Loss Expectancy (ALE) of a risk without controls is expected to be \$35,000 to a business process you are evaluating. You are recommending a control that will save 80 percent of that loss at an annual cost of \$20,000 over the life of the process. Is the control justifiable?

- A. No, the savings is insignificant and relative to the cost.
- B. Yes, 80 percent of the loss amounts to \$28,000 per year, which exceeds the annual cost by \$8,000 per year.
- C. No, ALE is a subjective number and cannot be depended on to make this decision.
- D. Maybe, it depends on the managements appetite for risk and loss.

Answer: B

The correct answer is B. This is a justifiable control mechanism for management to consider for implementation. The significance of the savings compared to the cost (A) is a management decision and not one the IS auditor should be making. While ALE may be somewhat subjective (C), if its source and the method used to derive it is objective and reliable, it is a valid way to determine potential saving or loss over time. While management does have the responsibility for making decisions related to implementing all controls (D), this is still a justifiable control, should management choose to implement it.

157. What is the most important aspect of risk analysis to keep in mind when reviewing a business process?

- A. Senior management must be held accountable for all risks to the business.
- B. All risks do not need to be eliminated for a business to be profitable.
- C. Risks must be identified and documented in order to perform proper analysis on them.
- D. Line management should be involved in the risk analysis because management sees risks daily that others would not recognize.

Answer: C

The correct answer is C. In order to manage and control a risk, it first must be recognized as a risk. This implies identifying and documenting all risks no matter how small to perform a rigorous analysis for the business risks. Only after the loss potential and frequency of occurrence have been determined can risk be prioritized for control and mitigation. The other answers are all valid, but this is the most important aspect of risk analysis of those mentioned here.

158. Before making a recommendation to management for the further mitigation of residual risk during a gap analysis in a risk assessment, the following considerations should be decided upon:

- I. Managements risk tolerance
- II. The best type of control for the risk scenario and the process
- III. The gap between the acceptable risk and the residual risk
- IV. The state of the art, best practice for the process being reviewed
- V. Additional risk mitigation that the proposed control would address for the process under review

- A. I, II, III, and V only
- B. II, III, and V only
- C. II, III, IV, and V only
- D. I, II, III, IV, and V

Answer: A

The correct answer is A. All of the items mentioned except for the processing best practice are part of a risk analysis gap assessment. It really does not matter if there is a better way to perform the processing unless a reengineering evaluation is part of the assessment. Risk and control assessment are intended to address existing processes and changing the process should not be a consideration when recommending additional controls to close the gaps between acceptable risk, defined by examining existing controls and managements definition of acceptable risk, and the current state of risk control in effect.

159. What is the primary reason for independent assurance as a requirement for relying on control assessment and evaluation?

- A. The review of controls by independent reviewers transfers some amount of the risk to the reviewing body or organization.
- B. IS auditors are more knowledgeable about risks and controls and are better suited to review them and determine their effectiveness.

- C. Unless the controls are reviewed by an independent and objective review process, the quality of the controls cannot be assured.
- D. Management needs to have independent assurance that the risks are managed effectively as part of their corporate governance requirement.

Answer: C

The correct answer is C. The primary reason to use independent assurance is to get a second opinion on the effectiveness and efficiency of the controls in mitigating the risks of the business. IS auditors (B) are only one way to get this second opinion and they may not be best suited to evaluate some of the controls. While reviewing and drawing conclusions has some risk in and of itself (A), the risks of the business cannot be transferred by the independent review process. Finally, corporate governance should require that management is accountable for managing the risks of the business as well, but this is not the primary reason for seeking independent assurance.

160. What are examples of additional risk to a business that third party may add to the overall risks of the business?

- A. None, a business will actually take on some of the risk and reduce the overall risks to the business.
- B. A business will take on the risk that they do not have proper processes in place to perform inefficiently.
- C. A business will take on the risks that the contractual commitments do not adequately compensate for poor performance of the third-party vendor.
- D. A business will take on the risk that the customers are impacted by missed service level commitments or the misuse of customer information.

Answer: D

The correct answer is D. Customer impact is an example of additional risk that cannot be contractually compensated for and will be added to the business by engaging third-party vendors as part of the business process. Engaging in business with third parties does not transfer managements accountability or responsibilities for risk (A). Inefficiency in the third parties business process (B) is not a risk for the host business. Contractually added risk (C) should be addressed when the contracts are negotiated and poor performance of the third party is one of the considerations that should be inputted to the negotiation and contract development process.