# Isaca

*CISA*
*Certified Information Systems Auditor*

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

# Total Questions: 1043
# Latest Version

## Question: 1

An IS auditor notes that help desk personnel are required to make critical decisions during major service disruptions. Which of the following is the auditor's BEST recommendation to address this situation?

A. Introduce classification of disruptions by risk category.
B. Provide historical incident response information for the help desk
C. Implement an incident response plan
D. Establish shared responsibility among business peers.

**Answer: C**

## Question: 2

A company has implemented an IT segregation of duties policy In a role-based environment, which of the following roles may be assigned to an application developer?

A. Database administration
B. Emergency support
C. IT operator
D. System administration

**Answer: D**

## Question: 3

Which of the following is the BEST source of information when assessing the amount of time a project will take?

A. Critical path analysis
B. Workforce estimate
C. GANT chart
D. Scheduling budget

**Answer: C**

## Question: 4

Which of the following is a passive attack on a network?

A. Sequence analysis
B. Traffic analysis
C. Message service interruption
D. Message modification

**Answer: B**

## Question: 5

What is the GREASTEST concern for an IS auditory reviewing contracts for licensed software that executes a critical business process?

A. The contract does not contain a right-to-audit clause.
B. Software escrow not negotiated.
C. Several vendor deliveries missed the commitment data.
D. An operational level agreement (OLA) was not negotiated.

**Answer: B**

## Question: 6

The IS auditor of a power company finds that the radio link to a remote mountain site is experience systematic outages under specific weather conditions. The communications managers explains that increasing the radio power would require a new license and would help. What is the MOST appropriate action by the IS auditor?

A. Recommend that the site s hardware be upgraded to record data during outages.
B. Gather additional information to identify threats vulnerabilities and impact.
C. Review the installation license, permissions and associated costs.
D. Recommend that the site's data collection and transmission be non-interruptible.

**Answer: B**

## Question: 7

Which of the following would be the MOST effective method to address software license violations on employee workstations?

A. Implementing real-time monitoring software on employee workstations
B. Restricting administrative rights on employee workstations
C. Scanning of workstation daily for unauthorized software use
D. Required automated installation of software.

**Answer: A**

## Question: 8

An IT governance body wants to determine whether IT service delivery is based on consistently efficient and effective processes. Which of the following would be the BEST approach?

A. Evaluate key performance indicators (KPis).
B. Conduct a gap analysis.
C. Analyze current and future capacity.
D. Implement a balanced scorecard

**Answer: A**

## Question: 9

When conducting a follow-up audit on an organization s firewall configuration, the IS auditor discovered that the firewall had been integrated into a new system that provides both firewall and intrusion detection capabilities. The IS auditor should:

A. review the compatibility of the new system with existing network controls
B. consider the follow-up audit unnecessary since the firewall is no longer being used
C. assess whether the integrated system addresses the identified risk
D. evaluate whether current staff is able to support the new system

**Answer: C**

## Question: 10

One advantage of monetary unit sampling is the fact that:

A. it increases the likelihood of selecting material items from the population,
B. large-value population items are segregated and audited separately
C. it can easily be applied manually when computer resources are not available

D. results are stated in terms of the frequency of items in error

**Answer: B**

## Question: 11

Which of the following could be used to evaluate the effectiveness of IT operations?

A. Total cost of ownership
B. Internal rate of return
C. Balanced scorecard
D. Net present value

**Answer: C**

## Question: 12

Which audit technique provides the GREATEST assurance that incident management procedures are effective?

A. Determining whether incidents are categorized and addressed
B. Comparing incident management procedures to best practices
C. Performing comprehensive vulnerability scanning and penetration testing
D. Evaluating end-user satisfaction survey results

**Answer: A**

## Question: 13

Two organizations will share ownership of a new enterprise resource management (ERM) system To help ensure the successful implementation of the system, it k MOST important to
define:

A. the governance model.
B. access to data.
C. appropriate procedures
D. custody of assets

**Answer: A**

## Question: 14

Which of the following is MOST helpful in preventing a systems failure from occurring when an application is replaced using the abrupt changeover technique?

A. Comprehensive testing
B. Comprehensive documentation
C. Threat and risk assessment
D. Change management

**Answer: D**

## Question: 15

Which of the following validation techniques would BEST prevent duplicate electronic vouchers?

A. Sequence check
B. Edit check
C. Cyclic redundancy check
D. Reasonless check

**Answer: A**

## Question: 16

Management decided to accept the residual risk of an audit finding and not take the recommended actions. The internal. Audit team believes the acceptance is inappropriate and has discussed the situation with executive management. After this discussion, there is still disagreement regarding the decision. Which of the following is the BEST course of action by internal audit.

A. Report the issue to the audit committee in a joint with execute management for resolution.
B. Schedule another meeting with executive management to convince them of taking action as recommended.
C. Document in the audit report that management has accepted the residual risk and take no further action.
D. Report this matter to the audit committee without notifying executive management.

**Answer: A**

## Question: 17

A disk management system's PRIMARY function is to:

A. Provide data on efficient disk usage.
B. Deny access to disk resident data files.
C. Monitor disk accesses for analytical review
D. Provide the method of control for disk usage

**Answer: D**

## Question: 18

Which of the following is the BEST way to facilitate proper follow-up for audit finding?

A. Conduct a surprise audit to determine whether remediation is in progress
B. Schedule a follow-up audit for two weeks after the initial audit was completed
C. Conduct a follow-up audit when findings escalate to incidents
D. Schedule a follow-up audit based on remediation due dates.

**Answer: B**

## Question: 19

Which of the following would be an appropriate role of internal audit in helping to establish an organization's privacy program?

A. Analyzing risks posed by new regulations
B. Developing procedures to monitor the use of personal data
C. Defining roles within the organization related to privacy
D. Designing controls to protect personal data

**Answer: B**

## Question: 20

Before concluding that internal controls can be relied upon, the IS auditor should:

A. document the system of internal control.
B. conduct tests of compliance
C. document application controls.
D. discuss the internal control weaknesses with the auditee

**Answer: B**

## Question: 21

An organization is in the process of deciding whether to allow a bring your own device (BYOD) program. If approved, which of the following should be the FIRST control required before implementation?

A. An accept able use policy
B. Device registration
C. Device baseline configurations
D. An awareness program

**Answer: A**

## Question: 22

An IS auditor has found that an organization is unable to add new servers on demand in a cost-efficient manner Which of the following is the auditor s BEST recommendation?

A. Upgrade hardware to newer technology.
B. Increase the capacity of existing systems.
C. Build a virtual environment
D. Hire temporary contract workers for the IT function.

**Answer: C**

## Question: 23

Which of the following is MOST likely to be prevented by a firewall connected to the Internet?

A. Disclosure of public key infrastructure (PKI) keys
B. Alteration of email message content
C. Dial-m penetration attacks
D. External spoofing of internal addresses

**Answer: D**

## Question: 24

An IS auditor reviewing the acquisition of new equipment would consider which of the following to be a significant weakness?

A. Evaluation criteria when finalized after the initial assessment of responses
B. Staff involved in the evaluation were aware of the vendors being evaluated.
C. Independent consultants prepared the request for proposal (RFP) documents.
D. The closing date for responses was extended after a request from potential vendors.

**Answer: A**

## Question: 25

A recent audit identified duplicate software licenses and technologies Which of the following would be MOST helpful to prevent this type of duplication in the future?

A. Conducting periodic inventory reviews
B. Updating IT procurement policies and procedures
C. Centralizing IT procurement and approval practices
D. Establishing a project management office

**Answer: C**

## Question: 26

Which of the following is the BEST approach to identify whether a vulnerability is actively being exploited?

A. Conduct a penetration test
B. Perform log analysis.
C. Review service desk reports.
D. Implement key performance indicators (KPIs).

**Answer: B**

## Question: 27

Which of the following is the BEST source for describing the objectives of an organization s information systems?

A. IT management
B. Business process owners
C. Information security management

D. End users

**Answer: B**

## Question: 28

Which of the following is MOST likely to enable a hacker to successfully penetrate a system?

A. Unpatched software
B. Decentralized dialup access
C. Lack of DoS protection
D. Lack of virus protection

**Answer: A**

## Question: 29

Which of the following should be the MOST important consideration when establishing data classification standards?

A. Reporting metrics are established.
B. An education campaign is established upon rollout.
C. The standards comply with relevant regulations.
D. Management supports the newly developed standards

**Answer: C**

## Question: 30

The operations team of an organization has reported an IS security attack. Which of the following should be the NEXT step for the security incident response team?

A. Perform a damage assessment
B. Report results to management.
C. Document lessons learned
D. Prioritize resources for corrective action

**Answer: D**

## Question: 31

The use of the Transport Layer Security (TLS) protocol enables the client in a network to be:

A. identified by a password.
B. assured of the server s identity.
C. registered by the server,
D. provided with a digital certificate

**Answer: D**

## Question: 32

An IS auditor has assessed a payroll service provider's security policy and finds significant topics are missing. Which of the following is the auditor's BEST course of action?

A. Recommend the service provider update their policy
B. Report the risk to internal management
C. Notify the service provider of the discrepancies.
D. Recommend replacement of the service provider

**Answer: B**

## Question: 33

Which of the following could an IS auditor recommend to improve the estimated resources required in system development?

A. Prototyping
B. Function point analysis
C. Business areas involvement
D. CASE tools

**Answer: D**

## Question: 34

A stockbroker accepts orders over the Internet. Which of the following is the MOST appropriate control to ensure confidentiality of the orders?

A. Public key encryption
B. Virtual private network
C. Digital signature

D. Data Encryption Standard (DES)

**Answer: B**

## Question: 35

The IS auditor has identified a potential fraud perpetrated by the network administrator. The IS auditor should:

A. share the potential audit finding with the security administrator.
B. issue a report to ensure a timely resolution.
C. review the audit finding with the audit committee prior to any other discussions
D. perform more detailed tests prior to disclosing the audit results.

**Answer: B**

## Question: 36

Which of the following procedures would BEST contribute to the reliability of information in a data warehouse?

A. Retaining only current data.
B. Maintain archive data
C. Maintaining current metadata
D. Storing only a single type of data

**Answer: C**

## Question: 37

Which of the following should be the PRIMARY reason to establish a social media policy for all employees?

A. To raise awareness and provide guidance about social media risks
B. To restrict access to social media during business hours to maintain productivity
C. To publish acceptable messages to be used by employees when posting
D. To prevent negative public social media postings and comments

**Answer: A**

## Question: 38

An organization has established hiring policies and procedures designed specifically to ensure network administrators are well qualified. Which type of control is in place?

A. Detective
B. Directive
C. Corrective
D. Preventive

**Answer: A**

## Question: 39

To help ensure the accuracy and completeness of end-user computing output it is MOST important to include strong:

A. documentation controls.
B. change management controls.
C. access management controls
D. reconciliation controls

**Answer: D**

## Question: 40

An audit committee is reviewing an annual IT risk assessment Which of the following is the BEST justification for the audits selected?

A. Underlying business risks
B. Applications impacted
C. Likelihood of an IT process failure
D. Key IT general process controls

**Answer: A**

## Question: 41

Which of the following is a key success factor for implementing IT governance?

A. Establishing an IT governance committee
B. Delivering IT projects within budget
C. Embedding quality assurance processes
D. Aligning IT and business strategies

**Answer: D**

## Question: 42

An IS auditor finds that a company is using a payroll provider hosted in a foreign country Of the following the MOST important audit consideration is whether the provider s operations;

A. meet industry best practice and standards
B. comply with applicable laws and regulations
C. are shared with other companies using the provider
D. are aligned with the company's culture

**Answer: B**

## Question: 43

To confirm integrity for a hashed message, the receiver should use

A. a different hashing algorithm from me sender s to create a binary image of the file
B. the same hashing algorithm as the tender s to create a numerical representation of the file.
C. a different hashing algorithm from the sender s to create a numerical representation of the file
D. the same hashing algorithm as the sender's to create a binary image of the file.

**Answer: D**

## Question: 44

Reviewing which of the following would be MOST helpful in assessing whether an organization s IT performance measures are comparable to other organizations in the same industry?

A. Maturity models for IT processes
B. Employee satisfaction surveys
C. Key performance indicators (KPIs) for IT processes
D. Reputable IT governance frameworks

**Answer: C**

## Question: 45

An IS auditor finds the timeliness and depth of information regarding the organization's IT projects varies based on which project manager is assigned. Which of the following recommendations would be A MOST helpful in achieving predictable and repeatable project management processes?

A. Alignment of project performance to pay incentives
B. Adoption of business case and earned value templates
C. Use of Gantt charts and work breakdown structures
D. Measurement against defined and documented procedures

**Answer: B**

## Question: 46

The FIRST step in establishing a firewall security policy is to determine the:

A. expected data Throughput.
B. business requirements,
C. existing firewall configuration,
D. necessary logical access rights

**Answer: B**

## Question: 47

While planning a security audit, an IS auditor is made aware of a security review carried out by external consultants. It is MOST implement for the auditor to:

A. Re-perform the security review
B. Asses the objectively and competence of the consultant
C. Review similar reports issued by the consultants.
D. Accept the finding and conclusion of the consultants

**Answer: C**

## Question: 48

Which of the following would be the MOST efficient audit approach, given that a compliance-based approach was adopted in the previous year?

A. Perform a review of significant transactions posted within the system
B. interview systems personnel to evaluate all automated controls
C. Evaluate the controls surrounding changes to programs.
D. Validate all applications using test data

**Answer: C**

## Question: 49

A security company and service provider have merged and the CEO has requested one comprehensive set of security policies be developed for the newly formed company. The IS auditor s BEST recommendation would be to:

A. implement the service provider's policies
B. implement the security company s policies,
C. adopt an industry standard security policy
D. conduct a policy gap assessment

**Answer: D**

## Question: 50

An organization offers an online information security awareness program to employees on an annual basis. Which of the following findings from an audit of the program should be the IS auditor's GREATEST concern?

A. Training completion is not mandatory for staff
B. New employees are given three months to complete the training.
C. The post-training test content is two years old.
D. Employees have complained about the length of the program

**Answer: A**

## Question: 51

The objective of using coding standards for systems development is to:

A. ensure that business needs are met
B. facilitate user testing

C. facilitate program maintenance
D. ensure the completeness of requirements.

**Answer: C**

## Question: 52

During a disaster recovery audit, an IS auditor finds that a business impact analysis (BIA) has not been performed The auditor should FIRST.

A. evaluate the impact on current disaster recovery capability.
B. issue an intermediate report to management
C. conduct additional compliance testing
D. perform business impact analysis

**Answer: B**

## Question: 53

Documentation of workaround processes to keep a business function operational during recovery of IT systems is a core part of a:

A. business continuity plan.
B. business impact analysis.
C. threat and risk assessment
D. disaster recovery plan

**Answer: B**

## Question: 54

Which of the following is an IS auditor s GREATEST concern when an organization does not regularly update software on individual workstations in the internal environment?

A. The organization may be more susceptible to cyber-attacks.
B. The organization may not be in compliance with licensing agreement.
C. System functionality may not meet business requirements.
D. The system may have version control issues.

**Answer: A**

## Question: 55

A bank is relocating its servers to a vendor that provides data center hosting services to multiple clients. Which of the following controls would restrict other clients from physical access to the bank servers?

A. Locking server cages
B. Biometric access at all data center entrances
C. 24-hour security guards
D. Closed-circuit television camera

**Answer: A**

## Question: 56

An IS auditor can BEST help management fulfill risk management responsibilities by:

A. ensuring the roles tor managing IT risk are defined
B. adopting a mechanism for reporting issues
C. highlighting specific risks not being addressed
D. developing an IT risk management framework

**Answer: C**

## Question: 57

An advantage of installing a thin client architecture in a local area network (LAN) is that this would:

A. stabilize network bandwidth requirements
B. reduce the risk of a single point of failure
C. facilitate the updating of software versions.
D. ensure application availability when the server is down.

**Answer: A**

## Question: 58

During a business process re-engineering (BPR) program, IT can assist with:

A. segregation of duties
B. streamlining of tasks

C. total cost of ownership,
D. focusing on value-added tasks.

**Answer: D**

## Question: 59

Which of the following BEST describes a common risk in implementing a new application software package?

A. Sensitivity of transactions is high
B. Transaction volume is excessive
C. The application lacks audit trails.
D. Parameter settings are incorrect

**Answer: D**

## Question: 60

Which of the following is corrective control?

A. Separating equipment development testing and production
B. Reviewing user access rights for segregation of duties
C. Verifying duplicate calculations in data processing
D. Executing emergency response plans

**Answer: D**

## Question: 61

Which of the following is MOST important to include in a contract to outsource data processing that involves customer personally identifiable information (Pit)?

A. The vendor must comply with the organization is legal and regulatory requirement.
B. The vendor must provide an independent report of its data processing facilities.
C. The vendor must compensate the organization if nonperformance occurs.
D. The vendor must sign a nondisclosure agreement with the organization.

**Answer: C**

## Question: 62

Which of the following should the IS auditor use to BEST determine whether a project has met its business objectives?

A. Earned-value analysis
B. Issues log with resolutions
C. Benefits realization document
D. Completed project plan

**Answer: C**

## Question: 63

Which of the following is the MOST important process to ensure planned IT system changes are completed in an efficient manner?

A. Incident management
B. Demand management
C. Release management
D. Configuration management

**Answer: C**

## Question: 64

When auditing a quality assurance plan, an IS auditor should be MOST concerned if the:

A. SDLC is coupled with the quality assurance plan
B. quality assurance function is periodically reviewed by internal audit
C. scope of quality assurance activities is undefined
D. quality assurance function is separate from the programming function

**Answer: C**

## Question: 65

The information security function in a large organization is MOST effective when:

A. partnered with the IS development team to determine access rights

B. decentralized as close to the user as possible
C. established at a corporate-wide level.
D. the function reports directly to the IS operations manager.

**Answer: C**

## Question: 66

Which of the following entities is BEST suited to define the data classification levels within an organization?

A. Business owner responsible for the respective data
B. Database administrator based on the data schema
C. System administrate responsible for data security controls
D. Legal compliance team based on the applicable regulations

**Answer: A**

## Question: 67

Following the sale of a business division, employees will be transferred to a new organization, but they will retain access to IT equipment from the previous employer. An IS auditor has recommended that both organizations agree to and document an acceptable use policy for the equipment. What type of control has been recommended?

A. Detective control
B. Directive control
C. Preventive control
D. Corrective control

**Answer: A**

## Question: 68

Which of the following will BEST help to ensure that an in-house application in the production environment is current?

A. Version control procedures
B. Change management
C. Production access control
D. Quality assurance

**Answer: A**

## Question: 69

An organization is replacing a mission-critical system. Which of the following is the BEST implementation strategy to mitigate and reduce the risk of system failure?

A. Stage
B. Phase
C. Parallel
D. Big-bang

**Answer: C**

## Question: 70

Which of the following would an IS auditor recommend as the MOST effective preventive control to reduce the risk of data leakage'

A. Ensure that paper documents arc disposed security.
B. Implement an intrusion detection system (IDS).
C. Verify that application logs capture any changes made.
D. Validate that all data files contain digital watermarks

**Answer: D**

## Question: 71

Assessments of critical information systems are based on a cyclical audit plan that has not been updated for several years. Which of the following should the IS auditor recommend to BEST address this situation?

A. Update the audit plan quarterly to account for delays and deferrals of period* reviews
B. Use a revolving set of audit plans to cover all systems
C. Do not include periodic reviews in detail as part of the audit plan.
D. Regularly validate the audit plan against business risks.

**Answer: D**

## Question: 72

An IS auditor has completed a service level management audit related to order management services provided by a third party Which of the following is the MOST significant finding?

A. The service level agreement does not define how availability is measured
B. Service desk support is not available outside the company s business hours
C. Penalties for missing service levels are limited.
D. The third party has offshore support arrangements.

**Answer: A**

## Question: 73

Which of the following would be an IS auditor's GREATEST concern when reviewing an organization s security controls for policy compliance?

A. End users are not required to acknowledge security policy training.
B. Security policy documents are available on a public domain website.
C. Buy-in from system owners to support the policies is inadequate
D. Security policies are not uniformly applicable across the organization

**Answer: C**

## Question: 74

An IS auditor is observing transaction processing and notes that a high-priority update job ran out of sequence. What is the MOST significant risk from this observation'

A. The job may not have run to completion.
B. Daily schedules may not be accurate
C. Previous jobs may have failed.
D. The job completes with invalid data.

**Answer: B**

## Question: 75

Which of the following controls will MOST effectively detect inconsistent records resulting from the lack of referential integrity in a database management system?

A. Concurrent access controls
B. Incremental data backups

C. Performance monitoring tools
D. Periodic table link checks

**Answer: D**

## Question: 76

During a review of information security procedures for disabling user accounts, an IS auditor discovers that IT is only disabling network access for terminated employees IT management maintains if terminated users cannot access the network, they will not be able to access any applications Which of the following is the GREATEST risk associated with
application access?

A. Loss of non-repudiation
B. Lack of segregation of duties
C. Inability to access data
D. Unauthorized access to data

**Answer: D**

## Question: 77

An IS auditor is examining a front-end sub ledger and a main ledger Which of the following would be the GREATEST concern if there are flaws in the mapping of accounts between the two systems?

A. Double-posting of a single journal entry
B. Inaccuracy of financial reporting
C. Unauthorized alteration of account attributes
D. inability to support new business Transactions

**Answer: B**

## Question: 78

Which of the following is the MOST significant risk associated with peer-to-peer networking technology?

A. Reduction in staff productivity
B. Loss of information during transmission
C. Lack of reliable internet network connections
D. Lack of central monitoring

**Answer: D**

## Question: 79

Which of the following access control situations represents the MOST serious control weakness?

A. Computer operators have access to system level flowcharts
B. Programmers have access to development hardware
C. System developers have access to production data
D. End users have access to program development tools.

**Answer: C**

## Question: 80

Which of the following should be done FIRST when planning a penetration test?

A. Execute nondisclosure agreements (NDAs).
B. Define the testing scope.
C. Determine reporting requirements for vulnerabilities
D. Obtain management consent for the testing

**Answer: A**

## Question: 81

Spreadsheets are used to calculate project cost estimates Totals for each cost category are then keyed into the job-costing system. What is the BIST control to ensure that data are accurately entered into the system?

A. Validity checks preventing entry of character data
B. Reconciliation total amounts by project
C. Display back of project detail after entry
D. Reasonableness checks for each cost type

**Answer: B**

## Question: 82

When developing a risk-based IS audit plan, the PRIMARY focus should be on functions:

A. with the most ineffective controls.
B. with the greatest number of threats.
C. considered critical to business operations.
D. considered important by IT management

**Answer: C**

## Question: 83

Which of the following would be MOST helpful when assessing how applications exchange data with other applications?

A. Results of a risk assessment on the applications
B. List of servers and their applications
C. Entity relationship diagram
D. Configuration management database

**Answer: C**

## Question: 84

Which of the following is the MOST important consideration for building resilient systems?

A. Eliminating single points of failure
B. Performing periodic backups
C. Creating disaster recovery plans
D. Defining recovery point objectives (RPOs)

**Answer: A**

## Question: 85

Which of the following would represent an acceptable test of an organization s business continuity plan?

A. Full test of computer operations at an emergency site
B. Paper test involving functional areas
C. Benchmarking the plan against similar organizations
D. Walk-through of the plan with technology suppliers

**Answer: B**

## Question: 86

An organization was recently notified by its regulatory body of significant discrepancies in its reporting dat
a. A preliminary investigation revealed that the discrepancies were caused by problems with the organization's data quality. Management has directed the data quality team to enhance their program The audit committee has asked internal audit to be advisors to the process. To ensure that management concerns are addressed, which data set should internal audit recommend be reviewed FIRST?
A. Data reported to the regulatory body
B. Data impacting business objectives
C. Data with customer personal information
D. Data supporting financial statements

**Answer: B**

## Question: 87

An intruder accesses an application server and makes changes to the system log. Which of the following would enable the identification of the changes?

A. Mirroring the system log on another server
B. Simultaneously duplicating the system log on a write-once disk
C. Write-protecting the directory containing the system log
D. Storing the backup of the system log offsite

**Answer: C**

## Question: 88

On a daily basis, an in-house development team moves duplicate copies of production data containing personally identifiable information (Pll) to the test environment Which of the following is the B€ST way to mitigate the privacy risk involved?

A. Require data owners to sign off on production data
B. Sanitize the data in the test environment
C. Encrypt the data file
D. Obtain customer opt-in acceptances.

**Answer: B**

## Question: 89

Which of the following is the MOST effective means of helping management and the IT strategy committee to monitor IT performance?

A. End-user satisfaction surveys
B. Gap analysis
C. Measurement of service levers against metrics
D. Infrastructure monitoring reports

**Answer: C**

## Question: 90

The MAJOR reason for segregating test programs from production programs is to:

A. provide control over program changes
B. limit access rights of IS staff to the development environment.
C. provide the basis for efficient system change management
D. achieve segregation of duties between IS staff and end users

**Answer: C**

## Question: 91

Due to system limitations, segregation of duties (SoD) cannot be enforced in an accounts payable system. Which of the following is the IS auditor s BEST recommendation for a compensating control?

A. Restrict payment authorization to senior staff members
B. Review payment transaction history.
C. Require written authorization for all payment transactions.
D. Reconcile payment transactions with invoices.

**Answer: C**

## Question: 92

Which of the following sampling techniques is commonly used in fraud detection when the expected occurrence rate is small and the specific controls are critical?

A. Random sampling
B. Discovery sampling
C. Monetary unit sampling
D. Stop-or-go sampling

**Answer: B**

## Question: 93

Which of the following is the BEST approach for performing a business impact analysis (BIA) of a supply-chain management application?

A. Reviewing me organization s policies and procedures
B. Circulating questionnaires to key internal stakeholders
C. Accepting IT personnel s view of business issues
D. Interviewing groups of key stakeholders

**Answer: D**

## Question: 94

To develop a robust data security program, the FIRST course of action should be to:

A. perform an inventory of assets.
B. implement data loss prevention controls.
C. interview IT senior management.
D. implement monitoring, controls

**Answer: A**

## Question: 95

Which of the following would BEST detect logic bombs in new programs?

A. Final acceptance testing by users
B. Parallel/pilot testing
C. Regression testing
D. Independent program review

**Answer: D**

## Question: 96

Which of the following will enable a customer to authenticate an online Internet vendor?

A. Customer verifies the vendor is certificate with a certificate authority (CA).
B. Vendor signs a reply using a hash function and the customer's public key.
C. Vendor decrypts incoming orders using its own private key.
D. Customer encrypts an order using the vendor s public key.

**Answer: B**

## Question: 97

A security review reveals an organization b struggling with a large number of findings from vulnerability scans. What should the IS auditor recommend be done FIRST.

A. Remediate vulnerabilities for the most critical systems
B. Conduct penetration tests to confirm critical findings.
C. Remediate issues that are rated as most critical
D. Address gaps for all internally developed applications

**Answer: C**

## Question: 98

Which of the following types of controls would BEST facilitate a root cause analysis for an information security incident?

A. Corrective
B. Preventive
C. Detective
D. Directive

**Answer: B**

## Question: 99

The maturity level of an organization s problem management support function is optimized when the function

A. has formally documented the escalation process.
B. proactively provides solutions
C. resolves requests in a timely manner
D. analyzes critical incidents to identify root cause.

**Answer: B**

## Question: 100

Which of the following would BEST enable an IS auditor to perform an audit that requires testing the full population of data?

A. Expertise in statistical sampling of data
B. Proficiency in the use of data analytics tools
C. Experience in database administration
D. Proficiency in programming and coding

**Answer: B**

## Question: 101

Which of the following is the GREATEST concern associated with migrating computing resources to a cloud virtualized environment?

A. An increase in inherent vulnerability
B. An increase in residual risk
C. An increase in the potential for data leakage
D. An increase in the number of e-discovery requests

**Answer: C**

## Question: 102

Which of the following protects against the impact of temporary and rapid decreases or increases in electricity?

A. Emergency power-off switch
B. Stand-by generator
C. Redundant power supply
D. Uninterruptible power supply (UPS)

**Answer: D**

## Question: 103

A company laptop has been stolen and all photos on the laptop have been published on social medi
a. Which of the following is the IS auditor's BEST course of action?
A. Determine if the laptop had the appropriate level of encryption
B. Verify the organization's incident reporting policy was followed
C. Ensure that the appropriate authorities have been notified
D. Review the photos to determine whether they were for business or personal purposes

**Answer: B**

## Question: 104

Which of the following is the BEST IS audit strategy?

A. Limit audits to new application system developments
B. Conduct general control audits annually and application audits in alternating years
C. Perform audits based on Impact and probability of error and failure.
D. Cycle general control and application audits over a two-year period

**Answer: C**

## Question: 105

During an external assessment of network vulnerability which of the following activities should be performed FIRST

A. implement an intrusion detection system (IDS)
B. Review policies
C. Monitor the network
D. Collect network information

**Answer: D**

## Question: 106

Which of the following provides the BEST evidence of the effectiveness of an organization s audit quality management procedures?

A. Quality of independent review scores
B. Number of resources dedicated to quality control procedures
C. Quality of auditor performance reviews
D. Number of audits completed within the annual audit plan

**Answer: A**

## Question: 107

Which of the following is the MOST significant driver of efficient handling of information security incidents?

A. Prioritization
B. Budget
C. Expertise
D. Strategy

**Answer: A**

## Question: 108

Which of the following would be the MOST likely reason for an intrusion prevention system (IPS) being unable to block an ongoing web attack?

A. Monitoring personnel are not proactive
B. The network design contains flaws.
C. Signatures are outdated
D. The firewall is not configured property.

**Answer: C**

## Question: 109

An IS auditor is using data analytics in an audit and has obtained the data to be used for testing. Which of the following is the MOST important task before testing begins?

A. Verify data analytics test scripts
B. Select the analytical sampling model
C. Document the source and method used to obtain the data
D. Verify the completeness and accuracy of the data

**Answer: C**

## Question: 110

Which of the following BEST provides continuous availability of network bandwidth for critical application services?

A. Configuration management
B. Quality of service (QoS)
C. Cloud computing
D. Problem management

**Answer: B**

## Question: 111

An organization was recently notified by its regulatory body of significant discrepancies in its reporting data. A preliminary investigation revealed that the discrepancies were caused problems with the organization's data quality. Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be visors to the process. After the data quality team identifies the system data at fault which of the following should internal audit recommend as the NEXT step m the process?

A. Identity the source data owners
B. Identify the root cause of data quality problems
C. Create business rules that validate data quality
D. Develop an improvement plan.

**Answer: C**

## Question: 112

Which of the following is a substantive test procedure?

A. Test of invoice calculation process
B. verifying that appropriate approvals are documented m a sample of program changes
C. Using audit software to verify The total of an accounts receivable file
D. Observing that user IDs and passwords are required to sign on to the online system

**Answer: A**

## Question: 113

When reviewing backup policies, an IS auditor MUST verify that backup intervals of critical systems do not exceed which of the following?

A. Service level objective (SLO)
B. Recovery time objective (RTO)
C. Maximum acceptable outage (MAO)
D. Recovery point objective (RPO)

**Answer: D**

## Question: 114

An IS auditor observes that an organization s critical IT systems nave experienced several failures throughout the year. Which of the following is the BEST recommendation?

A. Perform a root cause analysis.
B. Implement redundant systems.
C. Contract for a hot site
D. Perform a disaster recovery test

**Answer: B**

## Question: 115

An organization implements a data loss prevention tool as a control to mitigate the risk of sensitive data leaving the organization via electronic mail. Which of the following would provide the BEST indication of adequate control design?

A. Management has formally approved the control design.
B. Rules enforced by the tool were based on the classification of the data.
C. Management presents evidence that data loss incidents have decreased.
D. Security administrators can demonstrate the functions of the tool

**Answer: B**

## Question: 116

Which of the following is MOST important for the improvement of an organization's incident response processes

A. Regular upgrades to incident management software
B. Ongoing incident response training for users
C. Post-event reviews by the incident response team
D. Periodic walk-through of incident response procedures

**Answer: C**

## Question: 117

A complex IS environment which of the following tasks should be performed by the data owner?

A. Test the validity of backup data
B. Perform data restoration when necessary.
C. Perform technical database maintenance.
D. Review data classifications periodically

**Answer: D**

## Question: 118

Which of the following should be an IS auditor's PRIMARY consideration when evaluating the development and design of a privacy program?

A. Information security and incident management practices
B. Industry practice and regulatory compliance guidance
C. Data governance and data classification procedures
D. Policies and procedures consistent with privacy guidelines

**Answer: D**

## Question: 119

During a help desk review, an IS auditor determines the call abandonment rate exceeds agreed-upon service levels. What conclusion can be drawn from this finding?

A. Help desk staff are unable to resolve a sufficient number of problems on the first call.
B. There is insufficient staff to handle the help desk call volume.
C. Users are finding solutions from alternative sources.
D. There are insufficient telephone lines available to the help desk.

**Answer: B**

## Question: 120

Which of the following should be an IS auditor's FIRST activity when planning an audit?

A. Identify proper resources for audit activities.
B. Gain an understanding of the area to be audited.
C. Create a list of key controls to be reviewed.
D. Document specific questions in the audit program

**Answer: B**

## Question: 121

Which of the following controls will BEST ensure that the board of directors receives sufficient information about IT?

A. The CIO reports on performance and corrective actions in a timely manner.
B. Board members are knowledgeable about IT and the CIO is consulted on IT issues.
C. The CIO regularly sends IT trend reports to the board.
D. Regular meetings occur between the board the CIO and a technology committee

**Answer: B**

## Question: 122

Which of the following would BEST facilitate the detection of internal fraud perpetrated by an individual?

A. Mandatory leave
B. Flexible time
C. Corporate fraud hotline
D. Segregation of duties

**Answer: A**

## Question: 123

Which of the following is MOST important when an incident may lead to prosecution?

A. Independent assessment
B. Timely incident detection
C. Impact analysis
D. Preservation of evidence

**Answer: D**

## Question: 124

Which of the following should be of concern to an IS auditor performing a software audit on virtual machines?

A. Applications have not been approved by the CFO.
B. Multiple users can access critical applications.
C. Software licensing does not support virtual machines.
D. Software has been installed on virtual machines by privileged users.

**Answer: C**

## Question: 125

When conducting a requirements analysis for a project, the BEST approach would be to:

A. prototype the requirements,
B. test operational deliverable
C. consult key stakeholders
D. conduct a control self-assessment

**Answer: A**

## Question: 126

What is the BEST population to select from when testing that programs are migrated to production with proper approval?

A. List of changes provided by application programming managers
B. Change advisory board meeting minutes
C. Completed change request forms
D. List of production programs

**Answer: D**

## Question: 127

When reviewing business continuity plan (BCP) test results, it is MOST important for the IS auditor to determine whether the test:

A. considers changes to the systems environment
B. follows up on activities that occurred since the previous test
C. assesses the capability to retrieve vital records.
D. verifies the ability to resume key business operations.

**Answer: D**

## Question: 128

Which of the following is the BEST reason for an organization to develop a business continuity plan?

A. To avoid the costs resulting from the failure of key systems and processes
B. To establish business un« prioritization of systems projects, and strategies
C. To develop a detailed desertion of information systems and processes
D. To identify the users of information systems and processes

**Answer: B**

## Question: 129

MOST critical security weakness of a packet level firewall is that it can be circumvented by:

A. using a dictionary attack of encrypted passwords.
B. deciphering the signature information of the packets
C. intercepting packets and viewing passwords sent in clear text
D. changing the source address on incoming packets

**Answer: B**

## Question: 130

An IS auditor has discovered that unauthorized customer management software was installed on a workstation. The auditor determines the software has been uploading customer ita to an external party. Which of the following is the IS auditor's BEST course of action?

A. Determine the number of customer records that were uploaded
B. Notify the incident response team.
C. Review other workstations to determine the extent of the incident
D. Present the issue at the next audit progress meeting

**Answer: B**

## Question: 131

Which of the following is the MOST effective mechanism for ensuring that critical IT operational problems are reported to executive management in a timely manner?

A. Escalation procedures
B. Service level monitoring
C. Regular meetings
D. Periodic status reports

**Answer: A**

## Question: 132

During an audit, it is discovered that several suppliers with standing orders have been deleted from the supplier master file Which of the following controls would have BEST evented such an occurrence?

A. Existence check
B. Table look-ups
C. Logical relationship check
D. Referential integrity developed

**Answer: C**

## Question: 133

Which of the following provides the MOST assurance that a newly developed web application does not have IT security issues?

A. Server hardening

B. Penetration testing
C. Business impact analysts (BIA)
D. Application whitelisting

**Answer: B**

## Question: 134

MOST effective way to determine if IT is meeting business requirements is to establish:

A. a capability model.
B. industry benchmarks
C. key performance indicators (KPIs).
D. organizational goals.

**Answer: C**

## Question: 135

Which of the following observations noted during a review of the organization s social media practices should be of MOST concern to the IS auditor?

A. The organization does not require approval for social media posts.
B. Not all employees using social media have attended the security awareness program.
C. The organization does not have a documented social media policy.
D. More than one employee is authorized to publish on social media on behalf of the organization

**Answer: C**

## Question: 136

.. Implementing which of the following would BEST address issues relating to the aging of IT systems?

A. IT project management
B. Configuration management
C. Application portfolio management
D. Release management

**Answer: C**

## Question: 137

Which of the following would be MOST important for an IS auditor to review during an audit of an automated continuous monitoring process being used by the finance department.

A. Resiliency of the monitoring service
B. Configuration of the monitoring tool
C. Management sign-off of test documentation
D. Dual control and approvals embedded in processes

**Answer: A**

## Question: 138

Which of the following should be the PRIMARY consideration when developing an IT strategy?

A. Alignment with the IT investment portfolio
B. IT key performance indicators based on business objectives
C. Short and long-term plans for the enterprise IT architecture
D. Alignment with overall business objectives

**Answer: A**

## Question: 139

Which of the following should be of GREATEST concern to an IS auditor reviewing the controls for a continuous software release process?

A. Release documentation is not updated to reflect successful deployment
B. Testing documentation is not attached to production releases.
C. Developers are able to approve their own releases
D. Test libraries have not been reviewed in over six months

**Answer: C**

## Question: 140

Which of the following is the BEST time for an IS auditor to perform hich of the following is the BEST way to protect the confidentiality of data on a corporate smartphone?

A. Using encryption
B. Using remote data wipe capabilities
C. Disabling public wireless connections
D. Changing the default PIN for Bluetooth connections

**Answer: A**

## Question: 141

Which of the following is the BEST time for an IS auditor to perform a post-implementation review?

A. Before decommissioning the legacy system
B. Immediately after the new system goes into production
C. After the completion of user testing
D. When the system has stabilized

**Answer: D**

## Question: 142

An IS auditor has been asked to perform a post-implementation assessment of a new corporate human resources (HR) system. Which of the following control areas would be OST important to review for the protection of employee information?

A. Authentication mechanisms
B. Logging capabilities
C. System architecture
D. Data retention practices

**Answer: A**

## Question: 143

An airlines online booking system uses an automated script that checks whether fares are within the defined threshold of what is reasonable before the fares are displayed on the website. Which type of control is in place?

A. Preventer control
B. Corrective control
C. Detective control
D. Compensating control

**Answer: A**

## Question: 144

An IS audit manager finds that data manipulation logic developed by the audit analytics team leads to incorrect conclusions This inaccurate logic is MOST likely an indication of lich of the following?

A. Poor change controls over data sets collected from the business
B. The team's poor understanding of the business process being analyzed
C. Poor security controls that grant inappropriate access to analysis produced
D. Incompatibility between data volume and analytics processing capacity

**Answer: B**

## Question: 145

An IS auditor discovered that a firewall has more services than needed The IS auditor's FIRST recommendation should be to:

A. review configurations
B. deploy a network penetration team.
C. ensure logging is turned on.
D. Eliminate services except for HTTPS.

**Answer: A**

## Question: 146

Which of the following is the PRIMARY objective of the IS audit function?

A. Certify the accuracy of financial data
B. Facilitate extraction of computer-based data for substantive testing.
C. Perform reviews based on standards developed by professional organizations
D. Report to management on the functioning of internal controls.

**Answer: D**

## Question: 147

Which of the following is MOST important for an IS auditor to verify during a disaster recovery audit?

A. Regular backups are made and stored offsite.
B. Media are stored in fireproof cabmen.
C. Disaster recovery tests are carried out.
D. The disaster recovery plan is updated on a regular basis

**Answer: C**

## Question: 148

An IS auditor reviewing the use of encryption finds that the symmetric key is sent by an email message between the parties. Which of the following audit responses is correct in this situation?

A. No audit finding is recorded as it is normal to distribute a key of this nature in this manner
B. An audit finding is recorded as the key should be asymmetric and therefore changed
C. No audit finding is recorded as the key can only be used once
D. An audit finding is recorded as the key should be distributed in a secure manner

**Answer: D**

## Question: 149

Which of the following should be of MOST concern to an IS auditor reviewing an organization’s disaster recovery plan (DRP)?

A. Copies of the DRP are not kept in a secure offsite location.
B. The CIO has not signed off on the DRP
C. The disaster recovery steps are not detailed.
D. The responsibility for declaring a disaster is not identified

**Answer: D**

## Question: 150

Which of the following is an IS auditor's BEST course of action upon learning that preventive controls have been replaced with detective and corrective controls'

A. Report the issue to management as the risk level has increased.
B. Evaluate whether new controls manage the risk at an acceptable level.
C. Verify the revised controls enhance the efficiency of related business processes.
D. Recommend the implementation of preventive controls in addition to the other controls.

**Answer: B**

## Question: 151

Which of the following should the IS auditor do FIRST to ensure data transfer integrity for Internet of Things (IoT) devices?

A. Verify access control lists to the database where collected data is stored.
B. Determine how devices are connected to the local network.
C. Confirm that acceptable limits of data bandwidth are defined for each device.
D. Ensure that message queue telemetry transport (MQTT) is used.

**Answer: B**

## Question: 152

An organization has agreed to perform remediation related to high-risk audit findings. The remediation process involves a complex reorganization of user roles as well as the Implementation of several compensating controls that may not be completed within the next audit cycle Which of the following is the BEST way for an IS auditor to follow up on their activities?

A. Provide management with a remediation timeline and verity adherence
B. Schedule a review of the controls after the projected remediation date
C. Review the progress of remediation on a regular basis
D. Continue to audit the failed controls according to the audit schedule

**Answer: A**

## Question: 153

The MOST efficient way to confirm that an ERP system being implemented satisfies business expectations is to utilize which of the following types of testing?

A. Parallel
B. Sociability
C. Alpha
D. Pilot

**Answer: A**

## Question: 154

Which of the following data would be used when performing a business impact analysis (BIA)?

A. Cost benefit analysis of running the current business
B. Projected impact of current business on future business
C. Expected costs for recovering the business
D. Cost of regulatory compliance

**Answer: B**

## Question: 155

These members of an emergency incident response team should be:

A. restricted to IT personnel
B. appointed by the CISO
C. selected from multiple departments
D. assigned at the time of each incident

**Answer: C**

## Question: 156

An IS auditor is involved in the user testing phase of a development project. The developers wish to use a copy of a peak volume transaction file from the production process to should that the development can cope with the required volume What is the auditor s PRIMARY concern?

A. Users may not wish for production data to be made available for testing.
B. All functionality of the new process may not be tested.
C. Sensitive production data may be read by unauthorized persons.
D. The error-handling and credibility checks may not be fully proven

**Answer: C**

## Question: 157

An effective implementation of security roles and responsibilities is BEST evidenced across an enterprise when:

A. reviews and updates of policies are regularly performed
B. pokies are signed off by users.
C. operational activities are aligned with policies.
D. policies are rolled out and disseminated

**Answer: C**

## Question: 158

internal IS auditor recommends that incoming accounts payable payment files be encrypted. Which type of control is the auditor recommending?

A. Directive
B. Detective
C. Preventive
D. Corrective

**Answer: C**

## Question: 159

Which of the following features can be provided only by asymmetric encryption?

A. Data confidentiality
B. Information privacy
C. Nonrepudiation
D. 128-bit key length

**Answer: A**

## Question: 160

An organization plans to launch a social media presence as part of a new customer service campaign. Which of the following is the MOST significant risk from the perspective of potential litigation?

A. Approved employees can use personal devices to post on the company $ behalf
B. There is a lack of dear procedures for responding to customers on social media outlets
C. Access to corporate-sponsored social media accounts requires only single-factor authentication.
D. The policy stating what employees can post on the organization s behalf is unclear.

**Answer: D**

## Question: 161

Which of the following provides an IS auditor the MOST assurance that an organization is compliant with legal and regulatory requirements?

A. Senior management has provided attestation of legal and regulatory compliance
B. Controls associated with legal and regulatory requirements have been identified and tested
C. There is no history of complaints or fines from regulators regarding noncompliance
D. The IT manager is responsible for the organization s compliance with legal and regulatory requirements.

**Answer: B**

## Question: 162

When evaluating the recent implementation of an intrusion detection system (IDS), an IS auditor should be MOST concerned with inappropriate:

A. training
B. encryption
C. tuning
D. patching

**Answer: C**

## Question: 163

Which of the following BEST describes the relationship between vulnerability scanning and penetration testing?

A. For entities with regulatory drivers, the two tests must be the same
B. Both are labor-intensive in preparation, planning and execution.
C. Both utilize a risk-based analysis that considers threat scenarios.
D. The scope of both is determined primarily by the likelihood of exploitation

**Answer: C**

## Question: 164

An IS auditor is evaluating the log management system for an organization with devices and systems in multiple geographic locations. Which of the following is MOST important for e auditor to verify?

A. Log files w concurrently updated
B. Log files are encrypted and digitally signed.
C. Log files are reviewed in multiple locations.
D. Log files of the servers are synchronized.

**Answer: B**

## Question: 165

An IS auditor is a member of an application development team that is selecting software. Which of the following would impair the auditor's independence?

A. Approving the vendor selection methodology
B. verifying the weighting of each selection criteria
C. Reviewing the request for proposal (RFP)
D. Witnessing the vendor selection process

**Answer: A**

## Question: 166

Loss-site scripting (XSS) attacks are BEST prevented through:

A. a three-tier web architecture.
B. Secure coding practices
C. application firewall policy settings
D. use of common industry frameworks.

**Answer: B**

## Question: 167

Which of the following is the BEST indication of an effective incident management process?

A. Number of incidents reviewed by IT management
B. Percentage of incidents closed without escalation
C. Number of calls to the help des
D. Percentage of incidents where root cause has been identified

**Answer: B**

## Question: 168

An organization has implemented data storage hardware. Which of the following should an IS auditor review to assess if IT is maximizing storage and network utilization?

A. Downtime statistics
B. The quality management system
C. Routine and non-routine job schedules
D. Capacity management plans

**Answer: D**

## Question: 169

An IS auditor reviews change control tickets and finds an emergency change request where an IT manager approved the change, modified the code on the production platform, an solved the ticket Which of the following should be the auditor’s GREATEST concern?

A. There was no follow-up approval from the business
B. There was no testing prior to making the change in production
C. The IT manager performed the change and resolved the ticket
D. The change was made less than an hour after the request

**Answer: B**

## Question: 170

An IS auditor is conducting a review of an organization s information systems and discovers data that is no longer needed by business applications. Which of the following would b IS auditor's BEST recommendation?

A. Ask the data custodian to remove it after confirmation from the business user
B. Keep the data and protect it using a data classification policy
C. Assess the data according to the retention policy.
D. Back up the data to removable media and store in a secure area.

**Answer: D**

## Question: 171

Which of the following is a reason for implementing a decentralized IT governance model?

A. Standardized controls and economies of scale
B. Greater consistency among business units
C. Greater responsiveness to business needs
D. IT synergy among business units

**Answer: C**

## Question: 172

What is the FIRST step an auditor should take when beginning a follow-up audit?

A. Review workpapers from the previous audit
B. Review previous findings and action plans
C. Meet with the auditee to discuss remediation progress
D. Gather evidence of remediation to conduct tests of controls

**Answer: B**

## Question: 173

An IS auditor is conducting a review of a healthcare organization's IT policies for handling medical records. Which of the following is MOST important to verify?

A. IT personnel receive ongoing policy training.
B. Policy writing standards are consistent.
C. A documented policy approval process is in place.
D. The polices comply with regulatory requirements.

**Answer: D**

## Question: 174

Which of the following is the BEST way to address ongoing concerns with the quality and accuracy of internal audits?

A. Require IS audit management to lead exit meetings.

B. Require peer reviews of audit workpapers.
C. Engage an independent review of the audit function.
D. Implement performance management for IS auditors.

**Answer: C**

## Question: 175

Which of the following is MOST important to consider when creating audit follow-up procedures?

A. Whether follow-up procedures would determine if identified risks have been mitigated
B. Whether the auditee has allotted sufficient time for the follow-up
C. Whether management has determined if risk is within the organization's risk appetite
D. Whether the organization has sufficient funds to address the issue

**Answer: A**

## Question: 176

Which of the following would BEST indicate the effectiveness of a security awareness training program?

A. Increased number of employees completing training
B. Reduced unintentional violations
C. Results of third-parry social engineering tests
D. Employee satisfaction with trailing

**Answer: B**

## Question: 177

The PRIMARY advantage of object-oriented technology is enhanced:

A. management of sequential program execution for data access
B. management of a restricted variety of data types for a data object
C. grouping of objects into methods for data access
D. efficiency due to the re-use of elements of logic

**Answer: C**

## Question: 178

To help ensure the organization s information assets are adequately protected, which of the following considerations is MOST important when developing an information classification and handling policy?

A. The policy is owned by the head of information security, who has the authority to enforce the policy.
B. The policy has been mapped against industry frameworks for classifying information assets.
C. The policy specifies requirements to safeguard information assets based on their importance to the organization
D. The policy is subject to periodic reviews to ensure its provisions are up to date

**Answer: C**

## Question: 179

Which of the following approaches would utilize data analytics to facilitate the testing of a new account creation process?

A. Review new account applications submitted in the past month for invalid dates of birth
B. Evaluate configuration settings for the date of birth field requirements.
C. Review the business requirements document for date of birth field requirements.
D. Attempt to submit new account applications with invalid dates of birth

**Answer: C**

## Question: 180

An IS auditor conducting audit follow-up activities learns that some previously agreed-upon corrective actions have not been taken and that the associated risk has been accepted by senior management. If the auditor disagrees with management s decision what is the BEST way to address the situation?

A. Report the issue to the chief audit executive for resolution
B. Repeat the audit with audit scope only covering areas with accepted risks.
C. Take no action since management s decision has been made
D. Recommend new corrective actions to mitigate the accepted risk.

**Answer: A**

## Question: 181

An organization has software that is not compliant with data protection requirements. To help ensure that appropriate and relevant data protection controls are implemented in the future, the auditor s BEST course of action would be to:

A. map the organization's business processes to identify personally identifiable information (PII)
B. recommend an executive be appointed to oversee privacy program improvements.
C. recommend that privacy checks are included within the solution development life cycle.
D. conduct a privacy impact assessment to identify gaps in the organization's privacy practices

**Answer: D**

## Question: 182

Which of the following is BEST addressed when using a timestamp within a digital signature to deliver sensitive financial information?

A. Authentication
B. Nonrepudiation
C. Data integrity
D. Replay protection

**Answer: B**

## Question: 183

When reviewing an organization s IT governance processes, which of the following provides the BEST indication that information security expectations are being met at all levels?

A. Utilization of an internationally recognized security standard
B. Implementation of a comprehensive security awareness program
C. Approval of the security program by senior management
D. Achievement of established security metrics

**Answer: B**

## Question: 184

Which of the following an IS audit, which of the following types of risk would be MOST critical to communicate to key stakeholders?

A. inherent
B. Audit

C. Residual
D. Control

**Answer: C**

## Question: 185

Which of the following communication modes should be of GREATEST concern to an IS auditor evaluating end user networking?

A. Peer-to-peer
B. Client-to-server
C. Host-to-host
D. System-to-system

**Answer: A**

## Question: 186

While reviewing an organization s business continuity plan (BCP) an IS auditor observes that a recently developed application is not included. The IS auditor should:

A. ignore the observation as the application is not mission critical.
B. recommend that the application b# incorporated in the BCP.
C. ensure that the criticality of the application is determined
D. include m the audit findings that the BCP is incomplete

**Answer: C**

## Question: 187

Which of the following is the MOST important activity to undertake to avoid rework later in a project?

A. Acceptance testing
B. Risk assessment
C. Control review
D. Phase review

**Answer: D**

## Question: 188

maturity model is useful in the assessment of IT service management because it:

A. defines the level of control required to meet business needs
B. provides a benchmark for process improvement
C. specifies the mechanism needed to achieve defined service levels
D. indicates the service levels requited for the business area.

**Answer: B**

## Question: 189

An organization has established three IS processing environments: development, test, and production. The MAJOR reason for separating the development and test environments is

A. perform testing in a stable environment
B. obtain segregation of duties between IS staff and end users.
C. limit the users access rights to the test environment
D. protect the programs under development from unauthorized testing

**Answer: C**

## Question: 190

The grants management system is used to calculate grant payments. Once per day, a batch interface extracts grant amounts and payee details from this system for import into the once system so payments can be made overnight Which of the following controls provides the GREATEST assurance of the accuracy and completeness of the imported payment

A. Reconciling data from both systems
B. Restricting access to the grants and finance systems
C. Reviewing transaction logs for anomalies
D. Performing monthly bank reconciliations in a timely manner

**Answer: A**

## Question: 191

Which of the following would be MOST helpful in ensuring security procedures are followed by employees in a multinational organization?

A. Comprehensive end-user training
B. Security architecture review
C. Regular clean desk reviews
D. Regular policy updates by management

**Answer: A**

## Question: 192

An IS auditor begins an assignment and identifies audit components for which the auditor is not qualified to assess. Which of the following is the BEST course of anion?

A. Exclude the related tests from the audit plan and continue the assignment.
B. Notify audit management for a decision on how to proceed
C. Complete the audit and give full disclosure in the final audit report
D. Complete the work assignment to the best of the auditor's Ability

**Answer: B**

## Question: 193

While executing follow-up activities, an IS auditor is concerned that management has implemented corrective actions that are different from those originally discussed and agreed the audit function. In order to resolve the situation, the IS auditor/, BEST course of action would be to:

A. postpone follow-up activities and escalate the alternative controls to senior audit management
B. schedule another audit due to the implementation of alternative controls.
C. reject the alternative controls and re-prioritize the original issue as high risk.
D. determine whether the alternative controls sufficiently mitigate the risk and record the results

**Answer: D**

## Question: 194

During an IS audit, it is discovered that security configurations differ across the organization's virtual server farm. Which of the following is the IS auditor's BEST recommendation to proving the control environment?

A. Conduct a standard patch management review across the virtual server farm.

B. implement a security configuration baseline for virtual servers.
C. implement security monitoring controls for high-risk virtual servers
D. Conduct an independent review of each server s security configuration.

**Answer: B**

## Question: 195

Both statistical and nonstatistical sampling techniques:

A. permit the auditor to quantify and fix the level of risk
B. permit the auditor to quantity the probability of error,
C. provide each item an equal opportunity of being selected.
D. require judgment when defining population characteristics

**Answer: D**

## Question: 196

Which of the following is the BEST guidance from an IS auditor to an organization planning an initiative to improve the effectiveness of its IT processes?

A. IT management should include process improvement requirements in staff performance objectives
B. IT staff should be surveyed to identify current IT process weaknesses and suggest improvements.
C. The organization should refer to poor audit reports to identify the specific IT processes to be improved
D. The organization should use a capability maturity model to identify current maturity levels for each IT process.

**Answer: D**

## Question: 197

Which of the following is a detective control?

A. Echo checks m telecommunications
B. Programmed edit checks
C. A router rule restricting a service
D. Procedures for authorizing transactions

**Answer: B**

## Question: 198

Which of the following a recent internal data breach, an IS auditor was asked to evaluate information security practices within the organization. Which of the following findings would be MOST important to report to senior management?

A. Desktop passwords do not require special characters
B. Employees are not required to sign a non-compete agreement.
C. Users lack technical knowledge related to security and data protection
D. Security education and awareness workshops have not been completed

**Answer: D**

## Question: 199

mission-critical applications with a low recovery time objective (RTO). which of the following is the BEST backup strategy?

A. Archiving to conventional disk
B. Use of virtual tape libraries
C. Mirroring
D. Frequent back-ups to tape

**Answer: C**

## Question: 200

During an audit of information security procedures of a large retailer s online store, an IS auditor notes that operating system (OS) patches are automatically deployed upon -. Which of the following should be of GREATEST concern to the auditor?

A. Patches are not reflected in the configuration management database
B. Patches are in conflict with current licensing agreements
C. Patches are not tested before installation on critical servers.
D. Patches are pushed from the vendor increasing Internet traffic

**Answer: C**

## Question: 201

Overall responsibility for approving logical access rights to information assets should reside with the:

A. data and systems owners.
B. systems delivery and operations group
C. security administrator.
D. systems administrator.

**Answer: A**

## Question: 202

The BEST way to prevent fraudulent payments is to implement segregation of duties between payment processing and:

A. payment approval.
B. requisition creation.
C. vendor setup.
D. check creation.

**Answer: A**

## Question: 203

Which of the following metrics would be MOST helpful to an IS auditor in evaluating an organizations security incident response management capability?

A. Number of business interruptions due to IT security incidents per year
B. Number of malware infections in business applications detected per day
C. Number of alerts generated by intrusion detection systems (IDS) per minute
D. Number of IT security incidents reported per month

**Answer: A**

## Question: 204

Due to cost restraints, a company defers the replacement of hardware supporting core applications. Which of the following represents the GREATEST risk?

A. Eventual replacement may be more expensive.
B. future upgrades may not be possible.
C. Maintenance costs may rise

D. Systems availability may suffer.

**Answer: D**

## Question: 205

Outsourcing the development of business systems is MOST likely to result in the loss of:

A. accountability for end products
B. in-house competencies.
C. responsibility for IT security
D. control over strategic direction.

**Answer: C**

## Question: 206

Which of the following is the BEST way to control the concurrent use of licensed software?

A. Metering software
B. Monitor by system administrator
C. Surprise audit conducted by vendors
D. User self-discipline

**Answer: A**

## Question: 207

Following an unauthorized disclosure of data, an organization needs to implement data loss prevention (DLP) measures The IS auditor's BEST recommendation should be to:

A. install DLP software on corporate servers to prevent recurrence
B. monitor and block outgoing emails based on common DLP criteria,
C. restrict removable media access on all computer systems
D. establish a risk and control framework.

**Answer: D**

## Question: 208

Which of the following is the MOST effective control for a utility program?

A. Allowing only authorized personnel to use the program
B. Storing the program in a production library
C. Renaming the versions in the programmers libraries
D. Installing the program on a separate server

**Answer: A**

## Question: 209

During the procurement process which of the following would be the BEST indication that prospective vendors will meet the organization's needs?

A. service catalog is documented.
B. An account transition manager has been identified.
C. Expected service levels are defined
D. The vendor's subcontractors have been identified

**Answer: C**

## Question: 210

A post-implementation review of a system implementation has identified that the defined objectives were changed several times without the approval of the project board. What would the IS auditor do NEXT?

A. Determine whether the revised objectives are appropriate
B. Notify the project sponsor and request that the project be reopened.
C. Ask management to obtain retrospective approvals
D. Notify the project management office and raise a finding

**Answer: A**

## Question: 211

Which of the following analytical methods would be MOST useful when trying to identify groups with similar behavior or characteristics in a large population?

A. Classification
B. Correlation analysis
C. Clustering

D. Deviation detection

**Answer: B**

## Question: 212

Which of the following would be of MOST concern during an audit of an end-user computing system containing sensitive information?

A. Audit logging is not available
B. Secure authorization is not available
C. System data is not protected.
D. The system is not included in inventory.

**Answer: A**

## Question: 213

During a review of an insurance company s claims system, the IS auditor learns that claims for specific medical procedures are acceptable only from females This is an example of a:

A. logical relationship check
B. key verification.
C. completeness check.
D. reasonableness check

**Answer: B**

## Question: 214

An organization that has suffered a cyber attack is performing a forensic analysis of the affected users' computers Which of the following should be of GREATEST concern for the IS editor reviewing this process?

A. Audit was only involved during extraction of the information.
B. The legal department has not been engaged.
C. The chain of custody has not been documented
D. An imaging process was used to obtain a copy of the data from each computer.

**Answer: A**

## Question: 215

Which of the following would be the MOST effective method to identify high risk areas in the business to be included in the audit plan?

A. Review external audit reports of the business.
B. Review industry reports to identify common risk areas
C. Validate current risk from poor internal audit findings.
D. Engage with management to understand the business.

**Answer: D**

## Question: 216

Requiring that passwords contain a combination of numeric and alphabetic characters is MOST effective against which type of attack?

A. Dictionary
B. Denial of service
C. Social engineering
D. Programmed

**Answer: A**

## Question: 217

An IS auditor finds that firewalls are outdated and not supported by vendors. Which of the following should be the auditor s NEXT course of action?

A. Report the security posture of the organization.
B. Report the mitigating control
C. Determine the value of the firewall.
D. Determine the risk of not replacing the firewall

**Answer: B**

## Question: 218

Which of the following would MOST likely impact the integrity of a database backup?

A. Backing up the database to an optical disk
B. Relational database model used
C. Record fields contain null information
D. Open database files during backup

**Answer: D**

## Question: 219

..control that MOST effectively addresses the risk of piggybackingAailgating into a restricted area without a dead-man door is:

A. using two-factor authentication
B. security awareness training
C. requiring employees to wear ID badges
D. using biometric door locks.

**Answer: D**

## Question: 220

An internal audit department recently established a quality assurance (QA) program as part of its overall audit program. Which of the following activities is MOST important to rlude as part of the QA program requirements?

A. Implementing corrective action plans
B. Creating a long-term plan for internal audit staffing
C. Analyzing user satisfaction reports from business lines
D. Reviewing audit standards periodically

**Answer: C**

## Question: 221

An organization uses two data centers. Which of the following would BEST address the organization's need for high resiliency?

A. Each data center is recoverable via tape backups.
B. The data centers act as mirrored sites.
C. There is data replication across the data centers.
D. A hot site is used for the second site.

**Answer: B**

## Question: 222

The IS auditor's PRIMARY role in control self-assessment (CSA) is to:

A. evaluate the controls.
B. facilitate the process.
C. identify weaknesses
D. draw up an action plan.

**Answer: B**

## Question: 223

Which of the following is the PRIMARY advantage of using virtualization technology for corporate applications?

A. Increased application performance
B. Improved disaster recovery
C. Stronger data security
D. Better utilization of resources

**Answer: B**

## Question: 224

A small startup organization does not have the resources to implement segregation of duties. Which of the following would be the MOST effective compensating control?

A. Mandatory vacations
B. Rotation of log monitoring and analysis responsibilities
C. Additional management reviews and reconciliations
D. Third-party assessments

**Answer: B**

## Question: 225

What is the MOST important business concern when an organization is about to migrate a mission-critical application to a virtual environment?

A. Adequacy of the fallback procedures
B. Adequacy of the virtual architecture
C. The organization's experience with virtual applications
D. Confidentiality of network traffic

**Answer: A**

## Question: 226

Which of the following should be of GREATEST concern to an IS auditor reviewing actions taken during a forensic investigation?

A. The investigation report does not indicate a conclusion.
B. An image copy of the attacked system was not taken.
C. The proper authorities were not notified.
D. The handling procedures of the attacked system are not documented.

**Answer: C**

## Question: 227

Following significant organizational changes, which of the following is the MOST important consideration when updating the IT policy?

A. The policy is integrated into job descriptions.
B. The policy is endorsed by senior executives.
C. The policy is compliant with relevant laws and regulations.
D. The policy is aligned with industry standards and best practice.

**Answer: C**

## Question: 228

Which of the following is the GREATEST concern when an organization allows personal devices to connect to its network?

A. It is difficult To enforce the security policy on personal devices
B. It is difficult to maintain employee privacy.
C. IT infrastructure costs will increase.

D. Help desk employees will require additional training to support devices.

**Answer: A**

## Question: 229

An IS auditor evaluating a three-tier client/server architecture observes an issue with graphical user interface (GUI) tasks. Which layer should the auditor recommend the client address?

A. Presentation layer
B. Application layer
C. Storage layer
D. Transport layer

**Answer: A**

## Question: 230

Which type of control is being implemented when a biometric access device is installed at the entrance to a facility?

A. Preventive
B. Deterrent
C. Corrective
D. Detective

**Answer: C**

## Question: 231

Which of the following is the BEST physical security solution for granting and restricting access to individuals based on their unique access needs?

A. Bolting door locks
B. Cipher locks
C. Closed-circuit television (CCTV)
D. Electronic badge system

**Answer: D**

## Question: 232

An IS audit report highlighting inadequate network internal controls is challenged because no serious incident has ever occurred. Which of the following actions performed during the audit would have BEST supported the findings?

A. Compliance testing
B. Threat risk assessment
C. Penetration testing
D. Vulnerability assessment

**Answer: D**

## Question: 233

An IS auditor is performing a post-implementation review of a system deployed two years ago. Which of the following findings should be of MOST concern to the auditor?

A. Maintenance costs were not included in the project lifecycle costs.
B. Benefits as stated in the business case have not been realized.
C. Workarounds due to remaining defects had to be used longer than anticipated.
D. The system has undergone several change requests to further extend functionality.

**Answer: B**

## Question: 234

Which of the following methods should be used to purge confidential data from write-once optical media?

A. Degauss the media.
B. Destroy the media.
C. Remove the references to data from the access index.
D. Write over the data with null values.

**Answer: B**

## Question: 235

Which of the following should an IS auditor recommend as MOST critical to an effective performance improvement process for IT services?

A. Progress on performance goals is regularly reported to the board.
B. The performance goals are aligned with a commonly accepted framework.
C. Root cause analysis of service issues is used to develop performance goals.
D. Management accepts accountability for achieving performance goals.

**Answer: D**

## Question: 236

In reviewing the IT strategic plan, the IS auditor should consider whether it identifies the:

A. major IT initiatives.
B. links to operational tactical plans.
C. allocation of IT staff.
D. project management methodologies used.

**Answer: B**

## Question: 237

During a review of system access, an IS auditor notes that an employee who has recently changed roles within the organization still has previous access rights. The auditor s NEXT step should be to:

A. determine the reason why access rights have not been revoked
B. recommend a control to automatically update access rights.
C. direct management to revoke current access rights.
D. determine if access rights are in violation of software licenses-

**Answer: C**

## Question: 238

Following an IS audit recommendation, all Telnet and File Transfer Protocol (FTP) connections have been replaced by Secure Socket Shell (SSH) and Secure File Transfer Protocol (SFTP). Which risk treatment approach has the organization adopted?

A. Acceptance
B. Mitigation
C. Transfer

D. Avoidance

**Answer: B**

## Question: 239

Which of the following is MOST important to ensure when planning a black box penetration test?

A. The test results will be documented and communicated to management.
B. Diagrams of the organization s network architecture are available.
C. The environment and penetration test scope have been determined.
D. The management of the client organization is aware of the testing.

**Answer: C**

## Question: 240

Which of the following human resources management practices BEST leads to the detection of fraudulent activity?

A. Background checks
B. Time reporting
C. Employee code of ethics
D. Mandatory time off

**Answer: D**

## Question: 241

Performance monitoring tools report that servers are significantly below their planned utilization. Which of the following would be the BEST recommendation?

A. Consolidate physical servers.
B. Review the capacity plan.
C. Deploy load balancing.
D. Reconfigure server settings.

**Answer: B**

## Question: 242

An IS auditor reviewing an incident management process identifies client information was lost due to ransomware attacks. Which of the following would MOST effectively minimize the impact of future occurrences?

A. Change access to client data to read-only.
B. Improve the ransomware awareness program.
C. Back up client data more frequently.
D. Monitor all client data changes.

**Answer: C**

## Question: 243

Which of the following would be the MOST effective control to mitigate unintentional misuse of authorized access?

A. Regular monitoring of user access logs
B. Annual sign-off of acceptable use policy
C. Security awareness training
D. Formalized disciplinary action

**Answer: C**

## Question: 244

Which of the following is the PRIMARY benefit of implementing configuration management for IT?

A. It helps audit in verifying IT conformance to business requirements.
B. It establishes the dependency of application systems with various IT assets.
C. It provides visibility to the overall function and technical attributes of IT assets.
D. It helps automate change and release management processes in IT.

**Answer: C**

## Question: 245

The independence of an IS auditor auditing an application is maintained if the auditor's role is limited to:

A. creating system specifications.
B. defining user requirements.
C. recommending system enhancements

D. designing access control rules.

**Answer: C**

## Question: 246

An organization allows its employees to use personal mobile devices for work. Which of the following would BEST maintain information security without compromising employee privacy?

A. Installing security software on the devices
B. Restricting the use of devices for personal purposes during working hours
C. Partitioning the work environment from personal space on devices
D. Preventing users from adding applications

**Answer: C**

## Question: 247

A company uses a standard form to document and approve all changes in production programs. To ensure that the forms are properly authorized, which of the following is the MOST effective sampling method?

A. Discovery
B. Monetary
C. Variable
D. Attribute

**Answer: A**

## Question: 248

Which of the following is the MOST significant risk associated with the use of visualization?

A. Insufficient network bandwidth
B. Single point of failure
C. Inadequate configuration
D. Performance issues of hosts

**Answer: D**

## Question: 249

Which of the following is the PRIMARY reason for an IS auditor to use computer-assisted audit techniques (CAATs)?

A. To efficiently test an entire population
B. To perform direct testing of production data
C. To conduct automated sampling for testing
D. To enable quicker access to information

**Answer: A**

## Question: 250

Which of the following occurs during the issues management process for a system development project?

A. Contingency planning
B. Impact assessment
C. Configuration management
D. Help desk management

**Answer: C**

## Question: 251

A security administrator should have read-only access for which of the following?

A. Router configuration
B. Password policy
C. Security logs
D. Services/daemons configuration

**Answer: C**

## Question: 252

An IS auditor is planning to audit an organization's infrastructure for access, patching, and change management. Which of the following is the BEST way to prioritize the systems?

A. Complexity of the environment
B. Criticality of the system
C. System hierarchy within the infrastructure
D. System retirement plan

**Answer: B**

## Question: 253

Which of the following is MOST likely to result from compliance testing?

A. Comparison of data with physical counts
B. Confirmation of data with outside sources
C. Identification of errors due to processing mistakes
D. Discovery of controls that have not been applied

**Answer: D**

## Question: 254

Which of the following would be the GREATEST concern to an IS auditor reviewing an IT outsourcing arrangement?

A. Several IT personnel perform the same functions as the vendor.
B. The contract does not include a renewal option.
C. Development of KPIs that will be used was assigned to the vendor.
D. Some penalties were waived during contract negotiations.

**Answer: C**

## Question: 255

Which of the following should be the PRIMARY consideration for IT management when selecting a new information security tool that monitors suspicious file access patterns?

A. Integration with existing architecture
B. Ease of support and troubleshooting
C. Data correlation and visualization capabilities
D. Ability to contribute to key performance indicator data

**Answer: A**

## Question: 256

Which of the following would BEST enable alignment of IT with business objectives?

A. Leveraging an IT framework
B. Completing an IT risk assessment
C. Adopting industry best practices
D. Monitoring key performance indicators (KPIs)

**Answer: D**

## Question: 257

Which of the following is the FIRST consideration when developing a data retention policy?

A. Determining the backup cycle based on retention period
B. Designing an infrastructure storage strategy
C. Identifying the legal and contractual retention period for data
D. Determining the security access privileges to the data

**Answer: C**

## Question: 258

When evaluating whether the expected benefits of a project have been achieved, it is MOST important for an IS auditor to review:

A. post-implementation issues.
B. quality assurance results.
C. the project schedule.
D. the business case.

**Answer: D**

## Question: 259

Which of the following will BEST ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

A. Maintaining system console logs in electronic format
B. Ensuring bisynchronous capabilities on all transmission lines
C. Using a database management system (DBMS) to dynamically back-out partially processed transactions
D. Rotating backup copies of transaction files off site

**Answer: B**

## Question: 260

Which of the following is the MOST likely cause of a successful firewall penetration?

A. Use of a Trojan to bypass the firewall
B. Loophole m firewall vendor's code
C. Virus infection
D. Firewall misconfiguration by the administrator

**Answer: D**

## Question: 261

Intrusion detection systems (IDSs) can:

A. substitute for a firewall.
B. compensate for weak authentication mechanisms
C. conduct investigations of attacks from within the network
D. provide information to enhance the security infrastructure.

**Answer: D**

## Question: 262

To BEST evaluate the effectiveness of a disaster recovery plan, the IS auditor should review the:

A. test plan and results of past tests.
B. plans and procedures in the business continuity plan
C. capacity of backup facilities.
D. hardware and software inventory.

**Answer: A**

## Question: 263

Which of the following is the GREATEST concern with conducting penetration testing on an internally developed application in the production environment?

A. The testing could create application availability issues.
B. The testing may identify only known operating system vulnerabilities.
C. The issues identified during the testing may require significant remediation efforts.
D. Internal security staff may not be qualified to conduct application penetration testing.

**Answer: A**

## Question: 264

Which of the following is the PRIMARY reason for database optimization in an environment with a high volume of transactions?

A. Improving availability
B. Maintaining integrity
C. Preventing data leakage
D. Improving performance

**Answer: D**

## Question: 265

Which of the following tasks should be performed during an organization's business continuity plan (BCP) test?

A. Evaluate the security at the offsite facility.
B. Review the coverage of insurance.
C. Assess the critical information retrieval capability.
D. Review the alternate processing site contract.

**Answer: C**

## Question: 266

When planning for the implementation of a new system, an organization will opt for a parallel run PRIMARILY to:

A. ensure that the system meets required user response time.
B. validate system processing.
C. facilitate the training of new personnel
D. verify that system interfaces were implemented.

**Answer: B**

## Question: 267

An IS auditor is conducting a pre-implementation review to determine a new system's production readiness. The auditor's PRIMARY concern should be whether:

A. benefits realization has been evidenced
B. there are unresolved high-risk items
C. the project adhered to the budget and target date.
D. users were involved in the quality assurance (QA) testing.

**Answer: B**

## Question: 268

When auditing the IT governance of an organization planning to outsource a critical financial application to a cloud vendor, the MOST important consideration for the auditor should be:

A. the cost of the outsourced system.
B. the inclusion of a service termination clause.
C. alignment with industry standards.
D. alignment with business requirements.

**Answer: D**

## Question: 269

An organization is choosing key performance indicators (KPIs) for its information security management. Which of the following KPIs would provide stakeholders with the MOST useful information about whether information security risk is being managed?

A. Time from initial reporting of an incident to appropriate escalation
B. Time from identifying a security threat to implementing a solution
C. The number of security controls implemented
D. The number of security incidents during the past quarter

**Answer: B**

## Question: 270

A previously agreed-upon recommendation was not implemented because the auditee no longer agrees with the original finding. The IS auditor's FIRST course of action should be to:

A. exclude the finding in the follow-up audit report.
B. escalate the disagreement to the audit committee.
C. assess the reason for the disagreement.
D. require implementation of the original recommendation.

**Answer: C**

## Question: 271

An IS auditor has observed gaps in the data available to the organization for detecting incidents. Which of the following would be the BEST recommendation to improve the organization's security incident response capability?

A. Document procedures for incident escalation.
B. Document procedures for incident classification
C. Correlate security logs collected from multiple sources.
D. Centralize alerts and security log information.

**Answer: C**

## Question: 272

When reviewing the effectiveness of data center operations, the IS auditor would FIRST -stablish that system performance:

A. is monitored and reported against agreed service levels.
B. reflects the expected usage levels established at implementation.
C. meets the expected targets specified by the manufacturer.
D. is within generally accepted reliability levels for that system.

**Answer: A**

## Question: 273

An organization has purchased a replacement mainframe computer to cope with the demands of increased business. Which of the following should be the PRIMARY concern of an IS auditor?

A. The disaster recovery plan has been reviewed and updated.
B. Application access controls are adequate.
C. Appropriate tender evaluation processes have been followed.
D. The procurement is within the planned budget for the year.

**Answer: D**

## Question: 274

Which of the following would provide the MOST reliable evidence to indicate whether employee access has been deactivated in a timely manner following termination?

A. Comparing termination forms with dates in the HR system
B. Reviewing hardware return-of-asset forms
C. Interviewing supervisors to verify employee data is being updated immediately
D. Comparing termination forms with system transaction log entries

**Answer: D**

## Question: 275

An IS auditor is evaluating a virtual server environment and learns that the production server, development server, and management console are housed in the same physical host. What should be the auditor's PRIMARY concern?

A. The physical host is a single point of failure
B. The management console is a single point of failure.
C. The development server and management console share the same host
D. The development and production servers share the same host

**Answer: B**

## Question: 276

The GREATEST benefit of risk-based auditing is that it:

A. demonstrates compliance with regulatory requirements.
B. enables alignment of resources to significant risk areas.
C. allows an organization to identify and eliminate low-risk areas
D. identifies problem areas within an organization.

**Answer: B**

## Question: 277

Which of the following are BEST suited for continuous auditing?

A. Manual transactions
B. Irregular transactions
C. Low-value transactions
D. Real-time transactions

**Answer: B**

## Question: 278

To maintain the confidentiality of information moved between office and home on removable media, which of the following is the MOST effective control?

A. Mandatory file passwords
B. Security awareness training
C. Data encryption
D. Digitally signed media

**Answer: C**

## Question: 279

A review of Internet security disclosed that users have individual user accounts with Internet service providers (ISPs) and use these accounts for downloading business dat
a. The organization wants to ensure that only the corporate network is used. The organization should FIRST:
A. use a proxy server to filter out Internet sites that should not be accessed.
B. keep a manual log of Internet access.
C. monitor remote access activities.
D. include a statement in its security policy about Internet use.

**Answer: A**

## Question: 280

An organization s data retention policy states that all data will be backed up, retained for 10 years, and then destroyed. When conducting an audit of the long-term offsite backup program, an IS auditor should:

A. verify that business owners review data before it is destroyed.
B. verify that there is a process to ensure readability and restore capability
C. confirm that business interruption insurance coverage is in place.
D. review data classification schemes for appropriate security levels.

**Answer: B**

## Question: 281

Which of the following is MOST important for an IS auditor to do during an exit meeting with an auditee?

A. Ensure that the facts presented in the report are correct.
B. Specify implementation dates for the recommendations.
C. Request input in determining corrective action.
D. Communicate the recommendations to senior management

**Answer: B**

## Question: 282

Which of the following should be of GREATEST concern to an IS auditor conducting an audit of incident response procedures?

A. End users have not completed security awareness training.
B. Senior management is not involved in the incident response process.
C. There is no procedure in place to learn from previous security incidents.
D. Critical incident response events are not recorded in a centralized repository.

**Answer: B**

## Question: 283

An IS auditor finds that confidential company data has been inadvertently leaked through social engineering. The MOST effective way to help prevent a recurrence of this issue is to implement:

A. penalties to staff for security policy breaches
B. a third-party intrusion prevention solution
C. a security awareness program.
D. data loss prevention (DIP) software.

**Answer: C**

## Question: 284

An organization performs nightly backups but does not have a formal policy. An IS auditor should FIRST

A. evaluate current backup procedures.
B. document a policy for the organization.
C. recommend automated backup.
D. escalate to senior management.

**Answer: A**

## Question: 285

An IS auditor has completed a review of an outsourcing agreement and has communicating the issues at a meeting with senior management?

A. Present a completed report and discuss the details.
B. Provide a detailed report in advance and open the floor to questions.
C. Present an overview highlighting the key findings.
D. Provide a plan of action and milestones.

**Answer: A**

## Question: 286

Which of the following would be considered the BEST compensating control to use when an emergency process, rather than the established control procedures, is used for database changes?

A. Using an emergency user account with the access to make changes to the database
B. Using the administrator's own account to make out-of-hours changes
C. Logging detailed before-and-after images for later review by the administrator

D. Logging user's ID and change details for later review by the administrator

**Answer: D**

## Question: 287

What is the purpose of a hypervisor?

A. Monitoring the performance of virtual machines
B. Cloning virtual machines
C. Deploying settings to multiple machines simultaneously
D. Running the virtual machine environment

**Answer: D**

## Question: 288

An organization is developing data classification standards and has asked internal audit for advice on aligning the standards with best practices. Internal audit would MOST likely recommend the standards should be:

A. based on the results of an organization-wide risk assessment
B. based on the business requirements for confidentiality of the information.
C. aligned with the organization's segregation of duties requirements
D. based on the business requirements for authentication of the information.

**Answer: A**

## Question: 289

Which of the following would an IS auditor consider to be the MOST significant risk associated with a project to reengineer a business process?

A. The negative impact of change may not be documented.
B. The project manager is inexperienced in information systems.
C. Existing controls may be weakened or removed.
D. Existing baseline processes may not be reported to management.

**Answer: C**

## Question: 290

Which of the following is the FIRST step when conducting a business impact analysis?

A. identifying critical information resources
B. Identifying events impacting continuity of operations
C. Analyzing past transaction volumes
D. Creating a data classification scheme

**Answer: A**

## Question: 291

Which of the following findings would have the GREATEST impact on the objective of a business intelligence system?

A. Key controls have not been tested in a year.
B. Decision support queries use database functions proprietary to the vendor.
C. The hot site for disaster recovery does not include the decision support system.
D. Management reports have not been evaluated since implementation.

**Answer: A**

## Question: 292

Which of the following is the PRIMARY advantage of single sign-on (SSO)?

A. Improves system performance
B. Ensures good password practices
C. Improves security
D. Reduces administrative work load

**Answer: D**

## Question: 293

An accounting department uses a spreadsheet to calculate sensitive financial transactions. Which of the following is the MOST important control for maintaining the security of data in the spreadsheet?

A. There is a reconciliation process between the spreadsheet and the finance system.

B. The spreadsheet is locked down to avoid inadvertent changes.
C. A separate copy of the spreadsheet is routinely backed up.
D. Access to the spreadsheet is given only to those who require access.

**Answer: B**

## Question: 294

Which of the following is the PRIMARY concern if a business continuity plan (BCP) is not based on a business impact analysis (BIA)?

A. The critical systems were not identified but all systems are covered tn the BCP.
B. The knowledge of key people within the organization was not considered in the BCP.
C. The strategy of the BCP does not reflect estimated potential losses.
D. Management was not involved in the early stages of the BCP

**Answer: C**

## Question: 295

Which of the following BEST ensures that only authorized software is moved into a production environment?

A. Restricting read/write access to production code to computer programmers only
B. Assigning programming managers to transfer tested programs to production
C. A librarian compiling source code into production after independent testing
D. Requiring programming staff to move tested code into production

**Answer: C**

## Question: 296

In a follow-up audit, an IS auditor notes that management has addressed the original findings in a different way than originally agreed upon. The auditor should FIRST:

A. escalate the deviation to the audit committee.
B. mark the recommendation as satisfied and close the finding.
C. verify if management's action mitigates the identified risk
D. re-perform the audit to assess the changed control environment

**Answer: C**

## Question: 297

Which of the following is a detective control that can be used to uncover unauthorized access to information systems?

A. Requiring long and complex passwords for system access
B. Implementing a security information and event management (SIEM) system
C. Requiring internal audit to perform periodic reviews of system access logs
D. Protecting access to the data center with multif actor authentication

**Answer: B**

## Question: 298

Which of the following control checks would utilize data analytics?

A. Evaluating configuration settings for the credit card application system
B. Reviewing credit card applications submitted in the past month for blank data fields
C. Attempting to submit credit card applications with blank data fields
D. Reviewing the business requirements document for the credit card application system

**Answer: B**

## Question: 299

An e-commerce enterprise's disaster recovery (DR) site has 30% less processing capability than the primary site. Based on this information, which of the following presents the GREATEST risk?

A. Network firewalls and database firewalls at the DR site do not provide high availability.
B. No disaster recovery plan (DRP) testing has been performed during the last six months.
C. The DR site is in a shared location that hosts multiple other enterprises.
D. The DR site has not undergone testing to confirm its effectiveness.

**Answer: D**

## Question: 300

Which of the following is the BEST way to help ensure the security of privacy-related data stored by an organization?

A. Encrypt personally identifiable information.
B. Publish the data classification scheme.
C. Inform data owners of the purpose of collecting information.
D. Classify privacy-related data as confidential

**Answer: D**

## Question: 301

Which of ihe following is the BEST way to control scope creep during application system development?

A. Involve key stakeholders.
B. Implement project steering committee review.
C. Implement a quality management system.
D. Establish key performance indicators (KPIs).

**Answer: C**

## Question: 302

Which of the following controls is MOST appropriate against brute force attacks at login?

A. Storing password files using one-way encryption
B. Locking the account after three invalid passwords
C. Storing passwords under a one-way hash function
D. Increasing the minimum password length to 10 characters

**Answer: B**

## Question: 303

Which of the following is MOST important for an IS auditor to verify when reviewing a critical business application that requires high availability?

A. Algorithms are reviewed to resolve process ineffictencies.
B. Users participate in offsite business continuity testing.
C. There is no single point of failure.
D. Service level agreements (SlAs) are monitored.

**Answer: C**

## Question: 304

Which procedure provides the GREATEST assurance that corrective action to an audit report has been taken?

A. Performing subsequent audit tests to verify resolution of the deficiencies
B. Inquiring about the current status of the recommendation
C. Reporting to the audit committee or the board of directors concerning specific action taken or lack thereof
D. Requesting a written management reply to the audit report identifying corrective action for each deficiency

**Answer: A**

## Question: 305

Which of ihe following should be done FIRST to effectively define the IT audit universe for an entity with multiple business lines?

A. Identify aggregate residual IT risk for each business line.
B. Obtain a complete listing of the entity's IT processes
C. Obtain a complete listing of assets fundamental to the entity's businesses.
D. Identify key control objectives for each business line's core processes

**Answer: C**

## Question: 306

An IS auditor determines that a business continuity plan has not been reviewed and approved by management. Which of the following is the MOST significant risk associated with this situation?

A. Continuity planning may be subject to resource constraints.
B. The plan may not be aligned with industry best practice.
C. Critical business processes may not be addressed adequate.
D. The plan has not been reviewed by risk management

**Answer: C**

## Question: 307

A CIO has asked an IS auditor to implement several security controls for an organization s IT processes and systems. The auditor should:

A. obtain approval from executive management for the implementation
B. communicate the conflict of interest to audit management
C. perform the assignment and future audits with due professional care.
D. refuse due to independence issues.

**Answer: D**

## Question: 308

To effectively classify data, which of the following MUST be determined?

A. Data controls
B. Data ownership
C. Data users
D. Data volume

**Answer: B**

## Question: 309

An audit team has a completed schedule approved by the audit committee. After starting some of the scheduled audits, executive management asked the team to immediately audit an additional process. There are not enough resources available to add the additional audit to the schedule. Which of the following is the BEST course of action?

A. Revise the scope of scheduled audits.
B. Propose a revised audit schedule.
C. Approve overtime work to ensure the audit is completed.
D. Consider scheduling the audit for the next period.

**Answer: B**

## Question: 310

Which of the following is MOST important when planning a network audit?

A. Determination of IP range in use
B. Isolation of rogue access points

C. Identification of existing nodes
D. Analysts of traffic content

**Answer: B**

## Question: 311

Which of the following BEST helps to identify errors during data transfer?

A. Decrease the size of data transfer packets.
B. Test the integrity of the data transfer.
C. Review and verify the data transfer sequence numbers.
D. Enable a logging process for data transfer.

**Answer: C**

## Question: 312

For an organization which uses a VoIP telephony system exclusively, the GREATEST concern associated with leaving a connected telephone in an unmonitored public area is the possibility of:

A. theft of destruction of an expensive piece of electronic equipment.
B. unauthorized use leading to theft of services and financial loss,
C. network compromise due to the introduction of malware.
D. connectivity issues when used with an analog local exchange earner.

**Answer: C**

## Question: 313

Which of the following is the MOST important reason to use statistical sampling?

A. The results can reduce error rates.
B. It reduces time required for testing.
C. The results are more defensible •
D. It ensures that all relevant cases are covered.

**Answer: D**

## Question: 314

An organization is deciding whether to outsource its customer relationship management systems to a provider located in another country. Which of the following should be the PRIMARY influence in the outsourcing decision?

A. Time zone differences
B. The service provider's disaster recovery plan
C. Cross-border privacy laws
D. Current geopolitical conditions

**Answer: C**

## Question: 315

An organization is using a single account shared by personnel for its social networking marketing page. Which of the following is the BEST method to maintain accountability over the account?

A. Reviewing access rights on a periodic basis
B. Integrating the account with single sign-on
C. Regular monitoring of proxy server logs
D. Implementing an account password check-out process

**Answer: A**

## Question: 316

Which of the following is the MOST effective way to identify anomalous transactions when performing a payroll fraud audit?

A. Substantive testing of payroll files
B. Data analytics on payroll data
C. Observation of payment processing
D. Sample-based review of pay stubs

**Answer: B**

## Question: 317

Which of the following should be of MOST concern to an IS auditor during the review of a quality management system?

A. The quality management system includes training records for IT personnel.

B. Indicators are not fully represented in the quality management system.
C. There are no records to document actions for minor business processes.
D. Important quality checklists are maintained outside the quality management system.

**Answer: B**

## Question: 318

During an audit, which of the following would be MOST helpful in establishing a baseline for measuring data quality?

A. Built-in data error prevention application controls
B. Industry standard business definitions
C. Input from customers
D. Validation of rules by the business

**Answer: C**

## Question: 319

Which of ihe following BEST indicates a need to review an organization's information security policy?

A. Completion of annual IT risk assessment
B. Increasing complexity of business transactions
C. Increasing exceptions approved by management
D. High number of low-risk findings in the audit report

**Answer: B**

## Question: 320

Which of the following is a directive control?

A. Establishing an information security operations team
B. Updating data loss prevention software
C. Implementing an information security policy
D. Configuring data encryption software

**Answer: C**

## Question: 321

During a review of an application system, an IS auditor identifies automated controls designed to prevent the entry of duplicate transactions. What is the BEST way to verify that the controls work as designed?

A. Implement periodic reconciliations.
B. Review quality assurance (QA) test results.
C. Use generalized audit software for seeking data corresponding to duplicate transactions.
D. Enter duplicate transactions in a copy of the live system.

**Answer: D**

## Question: 322

A bank is selecting a server for its retail accounts application. To ensure that the server can handle a high volume of transactions with the required response times, which test should the IS auditor recommend?

A. Regression
B. Acceptance
C. Benchmark
D. Integration

**Answer: C**

## Question: 323

During an audit of an organization s incident management process, an IS auditor teams that the security operations team includes detailed reports of recent attacks in its communications to employees. Which of the following is the GREATEST concern with this situation?

A. Employees may fail to understand the seventy of the threats.
B. The reports may be too complex for a nontechnical audience.
C. Employees may misuse the information in the reports.
D. There is not a documented procedure to communicate the reports

**Answer: C**

## Question: 324

An organization's IT security policy requires annual security awareness training for all employees. Which of the following would provide the BEST evidence of the training's effectiveness?

A. Results of a social engineering lest
B. Interviews with employees
C. Decreased calls to the incident response team
D. Surveys completed by randomly selected employees

**Answer: A**

## Question: 325

Which type of risk would MOST influence the selection of a sampling methodology?

A. Control
B. Inherent
C. Residual
D. Detection

**Answer: A**

## Question: 326

What is the PRIMARY benefit of prototyping as a method of system development?

A. Reduces the need for testing.
B. Minimizes the time the IS auditor has to review the system.
C. Increases the likelihood of user satisfaction.
D. Eliminates the need for documentation.

**Answer: C**

## Question: 327

A large insurance company is about to replace a major financial application. Which of the following is the IS auditor's PRIMARY focus when conducting the pre-implementation review?

A. Procedure updates
B. Migration of data
C. System manuals
D. Unit testing

**Answer: B**

## Question: 328

To ensure confidentiality through the use of asymmetric encryption, a message is encrypted with which of the following?

A. Sender's private key
B. Recipient's private key
C. Sender's public key
D. Recipient's public key

**Answer: A**

## Question: 329

After an external IS audit, which of the following should be IT management's MAIN consideration when determining the prioritization of follow-up activities?

A. The scheduling of major changes in the control environment
B. The materiality of the reported findings
C. The availability of the external auditors
D. The amount of time since the initial audit was completed

**Answer: B**

## Question: 330

Which of the following should be an IS auditor’s PRIMARY consideration when evaluating the development and design of a privacy program?

A. Information security and incident management practices
B. Industry practice and regulatory compliance guidance
C. Policies and procedures consistent with privacy guidelines
D. Data governance and data classification procedures

**Answer: B**

## Question: 331

Which of the following provides the GREATEST assurance that any confidential information on a disk is no longer accessible but the device is still usable by the other internal users?

A. Erasing the disk
B. Degaussing the disk
C. Reformatting the disk
D. Password protecting the disk

**Answer: D**

## Question: 332

The BEST way to evaluate a shared control environment is to obtain an assurance report and review which of the following?

A. Master Service agreement
B. Service level agreement
C. Control self-assessment
D. Complementary user entity controls

**Answer: D**

## Question: 333

Privileged account access is require to start an ad hoc batch job. Which of the following would MOST effectively detect unauthorized job execution?

A. Introducing job execution request procedures
B. Executing the job through two-factor authentication
C. Requiring manual approval by an authorized users
D. Reconciling user activity logs against authorization

**Answer: D**

## Question: 334

An organization allows employees to use personally owned mobile devices to access customer's personal information. An IS auditor's GREATEST concern should be whether

A. Mobile devices are compatible with company infrastructure
B. Mobile device security policies have been implemented
C. Devices have adequate storage and backup capabilities

D. Devices have the capability to segregate business and personal data.

**Answer: B**

## Question: 335

Which of the following methodologies is MOST appropriate to use for developing software with incomplete requirements?

A. Agile
B. Waterfall
C. Critical chain
D. Process-based

**Answer: B**

## Question: 336

Which of the following is MOST important for an IS auditor to confirm when reviewing the effectiveness of an incident response program?

A. Incidents, are escalated to server management in a timely manner.
B. Incidents are categorized according to industry standards
C. Lessons learned are incorporated into incident response processes
D. The plan is reviewed and undated annually.

**Answer: C**

## Question: 337

An organization transmits large amount of data from one internal system to another. The IS auditor is reviewing quality of the data at the originating point. Which of the following should the auditor verify first?

A. The data has been encrypted
B. The data extraction process is completed
C. The data transformation is accurate
D. The source data is accurate

**Answer: D**

## Question: 338

An organization is running servers with critical business application that are in an area subject to frequent but brief power outages. Knowledge of which of the following would allow the organization's management to monitor the ongoing adequacy of the uninterruptable power supply (UPS)?

A. Number of servers supported by the ups
B. Duration and interval of the power outages
C. Business impact of server downtime
D. Mean time to recover servers after failure

**Answer: B**

## Question: 339

The demilitarized zone (DMZ) is the part of a network where servers that are placed are:

A. Running-mission critical, non-web application
B. Interacting with the public internet
C. Running internal department applications
D. External to the organization

**Answer: B**

## Question: 340

Which of the following should be of GREATEST concern to an IS auditor when auditing an organization's information security awareness

A. Training quizzes are designed and run by a third party company under a contract with the organization
B. The number of security incidents logged by employees to the help desk has increased in the past year
C. Security awareness training is run via the organization's enterprise wide e-learning portal
D. Security awareness training is not included as part of the on boarding process for new hires

**Answer: D**

## Question: 341

An IS auditor learns a server administration team regularly applies work arounds to address repeated failures of critical data processing services. Which of the following would BEST enable the organization to resolve the issue?

A. Change management
B. Incident management
C. Service level management
D. Problem management

**Answer: B**

## Question: 342

What is an IS auditor's BEST recommendation for management if a network vulnerability assessment confirms that critical patches have not been applied since the last assessment?

A. Implement a process to test and apply appropriate patches
B. Apply available patches and continue periodic monitoring
C. Configure servers to automatically apply available patches
D. Remove unpatched devices from the network

**Answer: A**

## Question: 343

Audit management has just completed the annual audit plan for the upcoming year, which consists entirely of high-risk processor. However it is determined that there are insufficient resources to execute the plan. What should be done NEXT?

A. Remove audit from the annual plan to better match the number of resources available.
B. Review the audit plan and defer some audits to the subsequent year
C. Present the annual plan to the audit committee and ask for more resources
D. Reduce the scope of the audit to better match the number of resources available

**Answer: C**

## Question: 344

Which of the following » the MOST important prerequisite for Implementing a data loss prevention (DLP) tool?

A. Developing a DLP policy and requiring signed acknowledgement by users.

B. Requiring users to save files in secured folders instead of company-wide shared drive
C. Identifying where existing data resides and establishing a data classification matrix.
D. Reviewing data transfer logs to determine historical patterns of data flow

**Answer: A**

## Question: 345

An is auditor discovers a recurring software control process issue that severely impacts the efficiency of a critical business process. Which of the following is the BEST recommendation?

A. Determine the root cause of the issue
B. Determine the compensating controls
C. Replace the malfunctioning system
D. Identity other impacted processes

**Answer: A**

## Question: 346

Which of the following is the BEST detective control for a job scheduling process involving data transmission?

A. Jobs are scheduled to be completed daily end data is transmitted using a secure Fife Transfer Protocol (FTP)
B. Job failure alerts are automatically generated and routed to support personnel
C. Metrics denoting the volume of monthly job failures are reported and reviewed by senior management
D. Jobs are scheduled and a log of this activity n retained for subsequent review

**Answer: A**

## Question: 347

Which of the following will MOST effectively help to manage the challenges associated with end user developed application systems?

A. Applying control practices used by IT
B. Introducing redundant support capacity
C. Developing classifications based on risk
D. Prohibiting creation of executable files

**Answer: C**

## Question: 348

An IS auditor identifies key controls that have been overridden by management. The next step the IS auditor should take is to

A. Perform procedures to quantify the irregularities
B. Withdraw from the engagement
C. Recommend compensating controls
D. Report the absence of key controls to regulators

**Answer: A**

## Question: 349

A 5 year audit plan provides for general audits every year and application audits on alternating years. To achieve higher efficiency, the IS audit manager would MOST likely:

A. Alternate between control self-assessment (CSA) and general audits every year.
B. Have control self-assessments (CSAs) and formal audits of application on alternating years
C. Implement risk assessment criteria to determine audit priorities
D. Proceed with the plan and integrate all new applications

**Answer: C**

## Question: 350

Based on the Guidance of internal audit, an IT steering committee is considering the use of a balanced scorecard to evaluate its project management process. Which of the following is the GREATEST advantage to using this approach?

A. Project scheduled and budget management will improve
B. Performance is measured from different perspectives
C. Information is provided m a consistent and timely manner.
D. Projects will be prioritized based on value

**Answer: B**

## Question: 351

An IS auditor reviewing security incident processes realizes incidents are resolved and dosed, but root causes are not investigated Which of the following should be the MAJOR concern with this situation?

A. Vulnerabilities have not been properly addressed
B. Lessons earned have not been property documented.
C. Abuses by employees have not been reported
D. Security incident policies are out of date

**Answer: A**

## Question: 352

During a routine check, a system administrator identifies unusual activity indicating an intruder within a firewall. Which of the following controls has MOST likely been compromised?

A. Data integrity
B. Identification
C. Authentication
D. Data validation

**Answer: C**

## Question: 353

Which of the following would be an auditor's GREATEST concern when reviewing data inputs from spreadsheets into the core finance system?

A. Undocumented code formats data and transmits directly to the database
B. There is not a complete inventory of spreadsheets, and file naming is inconsistent
C. Spreadsheets are accessible by all members of the finance department
D. The department data protection policy has not been reviewed or updated for two years

**Answer: C**

## Question: 354

During a software acquision review, an IS auditor should recommend that there be a software escrow agreement when:

A. There is no service level agreement (SLA)
B. The product is new in the market

C. The estimated life for the product is less than 3 years
D. The deliverables do not include the source code

**Answer: D**

## Question: 355

An IS auditor notes that the anticipated benefits from an ongoing infrastructure projects have changed due to recent organizational restructuring. Which of the following is the IS auditor's BEST recommendation?

A. Review and reapprove the business case
B. Review business goals and objectives
C. Conduct a new feasibility study
D. Review and update the business impact analysis (BIA)

**Answer: D**

## Question: 356

Which of the following is MOST important to include in forensic data collection and preservation procedure?

A. Preserving data integrity
B. Determining tools to be used
C. Assuring the physical security of devices
D. Maintaining chain of custody

**Answer: A**

## Question: 357

Which of the following is an example of audit risk?

A. Management may disagree with audit conclusions
B. Newer auditors may require additional supervision and training
C. Sampling methods may not detect a material error
D. Audit work may be lost due to a malware attack

**Answer: A**

## Question: 358

A user of a telephone banking system has forgotten his personal identification number (PIN), after the user has been authenticated, the BEST method of issuing a new pin is to have:

A. A randomly generated pin communicated by banking personnel
B. Banking personnel assign the user a new PIN via email
C. The user enter a new PIN twice
D. Banking personnel verbally assign a new PIN

**Answer: C**

## Question: 359

Which of the following is the most effective control for emergency changes to application programs?

A. Preparing and approving program change forms before the changes are made
B. Periodically checking the application program libraries to detect whether unauthorized changes have been made
C. Processing the change through change control with review of the change the following key
D. Keeping a sealed envelope containing a passwords that operator can use to make emergency changes

**Answer: B**

## Question: 360

Following a breach, what is the BEST source to determine the maximum amount of time before customers must be notified that their personal information may have been compromised?

A. Industry standards
B. Industry regulations
C. Incident response plan
D. Information security policy

**Answer: C**

## Question: 361

When introducing a maturity model to the IT management process, it is BEST to align the maturity level to a point that reflects which of the following?

A. Ideal business production level
B. Industry standard practice level
C. Minimum cost expenditure level
D. Maximum risk tolerance level

**Answer: D**

## Question: 362

Which of the following findings should hr of GREATEST concern for an IS auditor when auditing the effectiveness of a phishing simulation test administered for staff members?

A. Test results were not communicated to staff members
B. Staff members who failed the test did not receive follow-up education
C. Security awareness training was not provided poor to the test
D. Staff members were not notified about the test beforehand

**Answer: C**

## Question: 363

When reviewing a disaster recovery plan (DRP) an IS auditor should examine the:

A. Uninterruptible power supply (UPS)
B. Access to the computer site by the backup staff
C. Fire-fighting equipment
D. Offsite data file storage

**Answer: D**

## Question: 364

A review of an organization's IT portfolio revealed several applications that are not in use. The BEST way to prevent this situation from recurring would be to implement.

A. A formal request for proposal (RFP) process
B. Business case development procedures
C. An information asset acquisition policy
D. Asset life cycle management.

**Answer: D**

## Question: 365

An organization's plans to implement a virtualization strategy enabling multiple operating systems on a single host. Which of the following should be the GREATEST concern with this strategy?

A. Application performance
B. Network bandwidth
C. Adequate storage space
D. Complexity of administration

**Answer: D**

## Question: 366

Performance monitoring tools report that servers are consistently above the recommended utilization capacity. Which of the following is the BEST recommendation of the IS auditor?

A. Add servers until utilization is at target capacity
B. Monitor activity logs
C. Deploy load balancers
D. Develop a capacity plan based on usage projections

**Answer: B**

## Question: 367

Which of the following is the MOST significant concerns when backup tapes are encrypted?

A. Loss of encryption keys
B. Inaccurate data due to encryption processing
C. Incompatibility with future software versions
D. Lack of physical security over the tapes

**Answer: A**

## Question: 368

An organization globally distributes a free phone application that includes a module to gather and report user information. The application includes a privacy notice altering users to the data gathering. Which of the following presents the GREATEST risk?

A. There is no framework to delete personal data
B. The data is not properly encrypted on the application server
C. There may be a backlash among users when the data gathering is revealed
D. The data gathering notice is available in only one language

**Answer: B**

## Question: 369

An organization is considering outsourcing the processing of customer insurance claims. An IS auditor notes that customer data will be sent offshore for processing. Which of the following would be the BEST way to address the risk of exposing customer data?

A. Require background checks on service provider personnel involved in the processing of data.
B. Recommend the use of a service provide within the same country as the organization
C. Consider whether the service provider has the ability to meet service level agreements (SLA)
D. Assess whether the service provider meets the organization's data protection polices

**Answer: D**

## Question: 370

What is the MOST important role of a certificate authority (CA) when a private key becomes compromised?

A. Refresh the metadata of the certificates
B. Refresh the key information database is the certificate publishing server
C. Publish the certificate revocation lists (CRL) into the repository
D. Issue a new private key to the user

**Answer: C**

## Question: 371

During a review of an organization's network threat response process. The IS auditor noticed that the majority of alerts were closed without resolution. Management responded that those alerts were unworkable due to lack of actionable intelligence, and therefore the support team is allowed to close them. What is the best way for the auditor to address the situation?

A. Further review closed unactioned alerts to identify mishandling of threats
B. Omit the finding from the report as this practice is in compliance with the current policy
C. Recommend that management enhance the policy and improve threat awareness training
D. Reopen unactioned alerts and report to the audit committee

**Answer: A**

## Question: 372

An IS auditor determines that an online retailer processing credit card information does not have a data classification process. The auditor's NEXT step should be

A. Recommend the implementation of data loss prevention (DLP) tools.
B. Determine existing controls around sensitive data
C. Inquire if there have been any data loss incidents
D. Recommend encryption of all sensitive data as rest

**Answer: B**

## Question: 373

An organization has installed blade server technology in its data server. To determine whether higher cooling demands are maintained, which of the following should the IS auditor review?

A. Duct maintenance
B. Uninterruptable power supply (UPS) systems
C. Air conditioning capacity
D. Ventilation systems

**Answer: C**

## Question: 374

Which of the following should an IS auditor verify when auditing the effectiveness of virus protection?

A. Currency of software patch application
B. Frequency of external Internet access
C. Frequency of IDS log reviews
D. Schedule for migration to production

**Answer: A**

## Question: 375

The GREATEST risk of database renormalization is:

A. Decreased performance
B. Loss of database integrity
C. Incorrect metadata
D. Loss of data confidentiality

**Answer: A**

## Question: 376

In assessing the priority given to systems covered in an organization's business continuity plan (BCP), an IS auditor should FIRST:

A. Review the backup and restore process
B. Verify the criteria for disaster recovery site selection
C. Validate the recovery time objectives and recovery point objectives
D. Review results of previous business continuity plan (BCP) tests

**Answer: C**

## Question: 377

An IS auditor conducts a review of a third-party vendor's reporting of key performance indicators (KPI). Which of the following findings should be of MOST concern to the audition?

A. KPIs are not clearly defined
B. KPIs have never been updated
C. KPI data is not being analysed
D. Some KPIs are not documented

**Answer: B**

## Question: 378

Which of the following should be performed FIRST when preparing to deploy a major upgrade to a critical online application?

A. Update the disaster recovery process
B. Review data backup procedures
C. Update the business impact analysis (BIA)
D. Test the rollback process

**Answer: B**

## Question: 379

Which of the following is BEST for providing uninterrupted services?

A. Mirroring
B. Televaulting
C. Snapshots
D. Differential backup

**Answer: A**

## Question: 380

The quality assurance (QA) function should be prevented from

A. Developing naming conventions
B. Changing programs for business functions
C. Establishing analysis techniques
D. Amending review procedures

**Answer: B**

## Question: 381

Which of the following should be an IS auditor's GREATEST concern when evaluating a cybersecurity incident response plan?

A. Stakeholder contact details are not up to date
B. Rules and responsibilities are not detailed for each process
C. The plan has not been recently tested
D. The plan does not include incident response metrics

**Answer: D**

## Question: 382

Since data storage of a critical business application is on a redundant array of inexpensive disks (RAID). Backup are not considered essential. The IS auditor should recommend proper backup because RAID:

A. Relies on proper maintenance
B. Disks cannot be hot-swapped for quick recovery
C. Cannot offer protection against disk corruption
D. Cannot recover from a natural disaster

**Answer: D**

## Question: 383

The objectives of business process improvement should PRIMARILY include

A. Performance optimization
B. Changes of organizational boundaries
C. Minimal impact on staff
D. Incremental changes in productivity

**Answer: A**

## Question: 384

Which of the following should be reviewed as part of a data integrity test?

A. Confidentiality
B. Data backup
C. Redundancy
D. Completeness

**Answer: D**

## Question: 385

Which of the following is the MOST important consideration when deploying closed-circuit television (CCTV) systems that use wireless communication links to transmit images between cameras and a receiver?

A. Retention period of recordings
B. Encryption of transmission
C. Strategic placement of cameras
D. Monitoring by security guards

**Answer: B**

## Question: 386

Which of the following is the BEST compensating control for a lack of proper segregation of duties in an IT department?

A. Audit trail reviews
B. System activity logging
C. Authorization forms
D. Control self-assessment (CSA)

**Answer: A**

## Question: 387

An employee transfers from an organization's risk management department to become the lead IS auditor. While in the risk management department, the employee helped developed the key performance indicators (KPIs) now used by the organization. Which of the following would pose the GREATEST threat to the independence of this auditor?

A. Evaluating the effectiveness of IT risk management process
B. Developing KPIs to measure the internal audit team
C. Recommending controls to address the IT risks identified by KPIs
D. Training the IT audit team on IT risk management process

**Answer: A**

## Question: 388

An IS auditor would MOST likely recommend that IT management use a balanced scorecard to:

A. Assess IT functions and processes

B. Ensure that IT staff meet performance requirements
C. Indicate whether the organization meets quality standards
D. Train and educate IT staff

**Answer: B**

## Question: 389

Which of the following should an IS auditor recommend to reduce the likelihood of potential intruders using social engineering?

A. Prohibit the use of social networking platforms
B. Deploy a security awareness program
C. Perform simulated attacks
D. Implement an intrusion detection system (IDS)

**Answer: B**

## Question: 390

Which of the following would MOST effectively and executive management in achieving IT and business alignment?

A. Risk assessment
B. Balanced scorecard
C. Performance measurement
D. Value delivery assessment

**Answer: D**

## Question: 391

A vendor service level agreement (SLA) requires backup to be physically secured. An IS audit of the backup system revealed a number of the backup media were missing. Which of the following should be the auditor's NEXT step?

A. Notify executive management
B. Include the missing backup media finding in the audit report
C. Recommend identification of the data stored on the missing media
D. Recommend a review of the vendor's contract

**Answer: C**

## Question: 392

Which of the following findings should be an IS auditor's GREATEST concern when reviewing an organization's purchase of new IT infrastructure hardware?

A. The new infrastructure has compatibility issues with existing system
B. The new infrastructure has residual risk within the organization's risk tolerance
C. The new infrastructure's hardening requirements are stronger than required by policy
D. The new infrastructure arrived with default system settings

**Answer: A**

## Question: 393

Which of the following BEST enables timely detection of changes in the IT environment to support informed decision making by management?

A. Change management reports
B. Established key risk indicators (KRI)
C. Continuous monitoring
D. Sampling checks on high risk areas

**Answer: C**

## Question: 394

To test the integrity of the data in the accounts receivable master file, an IS auditor particularly interested in reviewing customers with balances over $400.000. the selection technique the IS auditor would use to obtain such a sample is called:

A. Systematic selection
B. Random selection
C. Stratification
D. Discovery sampling

**Answer: D**

## Question: 395

Which of the following should be of GREATEST concern to an IS auditor conducting an audit of an organization's backup processes?

A. The restoration process is slow due to connectivity issues.
B. The service level are not achieved
C. A written backup policy is not available
D. Backup failures are not resolved in a timely manner.

**Answer: C**

## Question: 396

Which of the following findings should be of MOST concern to an IS auditor when evaluating information security governance within an organization?

A. The information security department has difficulty filling vacancies
B. The data center manager has final sign-off on security projects
C. Information security policies were last updated two years ago
D. The information security oversight committee meets quarterly

**Answer: D**

## Question: 397

What would be an IS auditors GREATEST concern when using a test environment for an application audit?

A. Test and production environments do not mirror each other
B. Developers have access to the best environment
C. Test and production environments lack data encryptions
D. Retention period of test data has been exceeded

**Answer: A**

## Question: 398

As part of business continuity planning. Which of the following is MOST important to include in a business impact analyst (BIA)?

A. Define a risk appetite.
B. Assess risk of moving significant applications to the cloud

C. Assess recovery scenarios
D. Assess threats to the organization

**Answer: D**

## Question: 399

Which of the following metrics would BEST measure the agility of an organization's IT function?

A. Percentage of staff with sufficient IT related skills for the competency required of their roles
B. Frequency of security assessments against the most recent standards and guidelines
C. Average time to turn strategic. IT objectives into an agreed upon and approved initiative
D. Average number of learning and training hours per IT staff members

**Answer: B**

## Question: 400

Following a security breach, in which a hacker exploited a well-known vulnerability in the domain controller, an IS auditor has been asked to conduct a control assessment. The auditor's BEST course of action would be to determine it:

A. The network traffic was being monitored
B. The domain controller was classified for high availability
C. The logs were monitored
D. The patches were updated

**Answer: D**

## Question: 401

When reviewing a newly implemented quality management system (QMS), which of the following should be the IS auditor's PRIMARY concern?

A. The QMS post-implementation review (PIR) has not been finalized
B. The QMS testing methodology is not clearly documented
C. The QMS is not mapped to some core business processes
D. The QMS benefit measures were not included in the business case

**Answer: C**

## Question: 402

The PRIMARY advantage of object oriented technology is enhanced:

A. Efficiency due to the reuse of elements of logic
B. Management of sequential program execution for data access
C. Grouping of objects into methods for data access
D. Management of a restricted variety of data types for a data object

**Answer: A**

## Question: 403

An IS auditor is unable to directly test privacy controls for a client cloud based applications. The MOST effective alternative to direct testing is to review

A. Formal privacy certification
B. Independent audit reports
C. The provider's internal audit reports
D. The provider's statement of assurance

**Answer: B**

## Question: 404

After the release of an application system, an IS auditor wants to verify that the system is providing value to the organization. The auditor's BEST course of action would be to:

A. Quantify improvements in client satisfaction
B. Perform a gap analysis against the benefits defined in the business case
C. Review the results of compliance testing
D. Confirm that risk has declined since the application system release

**Answer: B**

## Question: 405

Which of the following is the MOST effective control to mitigate unintentional misuse of authorised access?

A. Formalized disciplinary action
B. Security awareness training
C. Annual sign-off of acceptable use policy
D. Regular monitoring of user access logs

**Answer: B**

## Question: 406

Which of the following is MOST important for an IS auditor to consider during a review of the IT governance of an organization?

A. Funding allocation
B. Defined service levels
C. Risk management methodology
D. Decision making responsibilities

**Answer: D**

## Question: 407

A recent audit concluded that an organization's information security system was weak and that monitoring would likely fail to detect penetration. Which of the following would be the MOST appropriate recommendation?

A. Identify and periodically remove sensitive data that is no longer needed
B. Look continually for new criminal behaviour and attacks on sensitive data
C. Encrypt sensitive data while strengthening the system
D. Establish a clear policy related to security and the handling of sensitive data

**Answer: C**

## Question: 408

During a security audit, which of the following is MOST important to review to ensure data confidentiality is managed?

A. Access log monitoring
B. Network configuration
C. Access controls
D. Data flows

**Answer: C**

## Question: 409

An IS auditor is analysing a sample of assesses recorded on the system log of an application. The auditor intends to launch an intensive investigation if one exception is found. Which sampling method would be appropriate?

A. Stratified sampling
B. Variable sampling
C. Judgemental sampling
D. Discovery sampling

**Answer: D**

## Question: 410

Which of the following provides the MOST comprehensive description of Its role in an organization?

A. IT job description
B. IT organizational chart
C. IT charter
D. IT project portfolio

**Answer: D**

## Question: 411

An organization considers implementing a system that uses a technology that is not in line with the organization's IT strategy. Which of the following is the BEST justification for deviating from the IT strategy?

A. The system makes use of state-of-the-art technology
B. The organization has staff familiar with the technology
C. The system has a reduced cost of ownership
D. The business benefits are achieved even with extra costs

**Answer: D**

## Question: 412

An IS auditor is assessing an organization's data loss prevention (DLP) solution for protecting intellectual property from insider theft. Which of the following would the auditor consider MOST important for effective data protection?

A. Creation of DLP policies and procedures
B. Encryption of data copied to flash drives
C. Employee training on information handling
D. Identification and classification of sensitive data

**Answer: D**

## Question: 413

Software quality assurance (QA) reviews are planned as part of system development. At which stage in the development process should the first review be initiated?

A. Immediately prior to user acceptance testing
B. During the feasibility study
C. At pre-implementation planning
D. As a part of the user requirements definition

**Answer: D**

## Question: 414

An employee loses a mobile device resulting in loss of sensitive corporate dat
a. Which of the following would have BEST prevented data leakage?
A. The triggering of remote data wipe capabilities
B. Complex password policy for mobile devices
C. Data encryption on the mobile device
D. Awareness training for mobile device users

**Answer: C**

## Question: 415

An IS auditor finds that the process for removing access for terminated employee is not documented. What is the MOST significant risk from this observation?

A. Access rights may not be removed in a timely manner
B. Unauthorized access cannot be identified

C. Procedures may not align with the practices
D. HR records may not match system access

**Answer: A**

## Question: 416

Which of the following should be an IS auditor's PRIMARY focus when developing a risk-banned IS audit program?

A. Business processes
B. IT strategic plans
C. Portfolio management
D. Business plans

**Answer: A**

## Question: 417

Which of the following it BEST enabled by following a configuration management process for new applications?

A. Maintaining adequate control over changes to production
B. Managing successful implementation of acquired software
C. Deploying approved emergence changes to production
D. Ensuring proper testing of code before deployment

**Answer: A**

## Question: 418

An IS auditor performing an audit of backup procedures observes that backup tapes are picked up weekly and stored offsite at a deed party hosting faculty. Which of the following recommendations would be the BEST way to maintain data integrity during transport?

A. Ensure the date is validated poor to transport
B. Ensure that logging and recording of data transport takes place
C. Ensure the transport company is licensed and assured.
D. Ensure the data is transported in locked tamper evident containers

**Answer: D**

## Question: 419

An IS auditor has discovered that a cloud-based application was not included in an application inventory that was used to confirm the scope of an audit. The business process owner explained that the application will be audited by a third party in the next year. The auditor's NEXT step should be to:

A. Evaluate the impact of the cloud application on the audit scope
B. Report the control deficiency to senior management
C. Revise the audit scope to include the cloud-based application
D. Review the audit report when performed by the third party

**Answer: B**

## Question: 420

Which of the following is the PRIMARY role of an IS auditor with regard to data privacy?

A. Drafting the organization's data privacy policy
B. Verifying that privacy practices match privacy statements
C. Ensuring compliance with data privacy laws
D. Communicating data privacy requirements to the organization

**Answer: C**

## Question: 421

An organization wants to test business continuity using a scenario in which there are many remote workers trying to access production data at the same time. Which of the following is the BEST testing method in this situation?

A. Application failover testing
B. Alternate site testing
C. Network penetration testing
D. Network sites testing

**Answer: C**

## Question: 422

The scheduling of audit follow-ups should be based PRIMARILY on

A. Control and detection processes
B. Costs and audit efforts involved
C. Auditee and auditor time commitments
D. The risk and exposure involved

**Answer: C**

## Question: 423

Which of the following would be MOST critical for an IS auditor to look for when evaluating fire precautions in a manned data center located in the upper floor of a multi-story building?

A. Documentation of tested emergency evacuation plans
B. Existence of handheld fire extinguishers in highly visible locations
C. Documentations of regular inspections by the local fire department
D. Adequacy of the HVAC system throughout the facility

**Answer: B**

## Question: 424

During a review of a production schedule, an IS auditor observes that a staff member is not complying with mandatory operational procedures. The auditor's NEXT step should be to:

A. Issue an audit memorandum identifying the incompliance
B. Include the noncompliance in the audit report
C. Determine why the procedures were not followed
D. Note the noncompliance in the audit working papers

**Answer: C**

## Question: 425

Due to the small size of the payroll department, an organization is unable to segregate the employee setup and payroll processing functions. Which of the following would be the BEST compensating control for the lack of segregation of duties?

A. An independent payroll disbursement review is conducted
B. The system is configured to require secondary approval for changes to the employee master file
C. A payroll variance report is reviewed tor anomalies every pay period

D. A review is conducted to verity that terminated employees, are removed from the employee master file.

**Answer: A**

## Question: 426

When conducting a post implementation review which of the following is the BEST way to determine whether the value from an IT project has been achieved?

A. Interview stakeholders
B. Calculate the return on investment (ROI)
C. Conduct an earned value analysis (EVA)
D. Survey and users

**Answer: C**

## Question: 427

In a typical SDLC, which group is PRIMARILY responsible for confirming compliance with requirements?

A. Risk management
B. Quality assurance
C. Steering committee
D. Internal audit

**Answer: B**

## Question: 428

Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceeding?

A. Documentation evidence handling by personnel throughout the forensic investigation
B. Engaging an independent third party to perform the forensic investigation
C. Restricting evidence access to professionally certified forensic investigation
D. Performing investigate procedures on the original hard drives rather than images of the hard drives

**Answer: A**

## Question: 429

When developing a business continuity plan (BCP) business unit management's involvement is MOST important during the

A. Implementation of a document repository
B. Development of business recovery procedures
C. Performance of an IS risk assessment
D. Performance of a business impact analysis (BIA)

**Answer: D**

## Question: 430

Which of the following should MOST concern an IS auditor reviewing an intrusion detection system (IDS)?

A. Number of false negatives
B. Legitimate traffic blocked by the system
C. Number of false positives
D. Reliability of IDS logs

**Answer: A**

## Question: 431

Which of the following is MOST important to include in an organization's incident response plan to help prevent similar incidents from happening in the future?

A. Containment and neutralization actions
B. Documentation of incident details
C. Incident closure procedures
D. Post-incident review

**Answer: D**

## Question: 432

Which of the following components of a scheduling tool BEST prevents job failures due to insufficient system resources?

A. Job dependencies
B. Exception handling
C. Error alerts
D. Delayed job starts

**Answer: B**

## Question: 433

While reviewing the project plan for a new system prior to go-live, an IS auditor notes that the project team has not documented a fallback plan. Which of the following would be the BEST go-live approach in this situation?

A. Parallel processing
B. Immediate cutover
C. Real-time replication
D. Load balancing

**Answer: A**

## Question: 434

Which of the following is the BEST indicator that an application system's agreed-upon level of service has been met?

A. Security Incident reports
B. CPU utilization reports
C. Transaction response time
D. Bandwidth usage logs

**Answer: A**

## Question: 435

When connecting to an organization's intranet from the Internet, security against unauthorized access is BEST achieved by using:

A. screening routers,
B. virtual private networks (VPNs).

C. proxy servers.
D. encryption

**Answer: A**

## Question: 436

An IS auditor has performed an agreed-upon procedures engagement for the organization's IT steering committee. Which of the following would be the MOST important element to include in the report?

A. Managements representation on the effectiveness of controls
B. An opinion on the effectiveness of controls
C. Statement that the engagement followed standards
D. Complementary user entity controls

**Answer: B**

## Question: 437

Which of the following attacks is BEST detected by an intrusion detection system (IDS)?

A. Logic bomb
B. Spoofing
C. System scanning
D. Spamming.

**Answer: B**

## Question: 438

Which of the following BEST describes an audit risk?

A. The financial report may contain undetected material errors.
B. The company is being sued for false accusations.
C. Employees have been misappropriating funds.
D. Key employees have not taken vacation for 2 years.

**Answer: D**

## Question: 439

An IS auditor performs a follow-up audit and learns the approach taken by the auditee to fix the findings differs from the agreed-upon approach confirmed during the last audit. Which of the following should be the auditor's NEXT course of action?

A. Evaluate the appropriateness of the rented s action taken.
B. Conduct a risk analysis incorporating the change.
C. Inform senior management of the change in approach.
D. Report results of the follow-up to the audit committee.

**Answer: A**

## Question: 440

An organization using development operations (DevOps) processes has deployed tools to provide automated configuration management functionality. Which of the following is the BEST way to ensure changes to system configuration do not inadvertently introduce security vulnerabilities into production platforms?

A. Implement automated scanning as part of the release process.
B. Implement logging of developer activity in the production environment.
C. Implement tools to inventory newly introduced application components.
D. Implement mechanisms for measuring production application performance.

**Answer: A**

## Question: 441

An IS auditor learns that after each scheduled batch process runs, management performs a reconciliation between upstream and downstream dat
a. Which of the following is MOST important for the auditor to investigate?
A. Change management over job scheduling
B. Results of user acceptance testing
C. Access to the job scheduler
D. Job failure resolution controls

**Answer: D**

## Question: 442

An IS auditor notes that several users have not logged into an application for more than one year. Which of the following would be the BEST audit recommendation?

A. Update the termination procedures
B. Delete the affected users' IDs.
C. Periodically review the information security policy.
D. Periodically review user access.

**Answer: D**

## Question: 443

An organization is currently replacing its accounting system. Which of the following strategies will BEST minimize risk associated with the loss of data integrity from the upgrade?

A. Parallel implementation
B. Functional integration testing
C. Fallback contingency
D. Pilot implementation

**Answer: A**

## Question: 444

An IS auditor is evaluating the risks and controls associated with a virtualized environment. Which of the following observations should be of GREATEST concern?

A. The change management process has not been updated to include virtualized environments.
B. Offline and dormant virtual machine Images are not patched on the same cycle as online ones.
C. The hypervisor’s security settings are not reviewed on a regular basis.
D. The hypervisor's partitioning resources have not been modified from its default settings.

**Answer: A**

## Question: 445

To achieve desired objectives, which of the following is MOST important to review when identifying potential areas of improvement in IT processes?

A. Past board minutes
B. Compliance activity trends
C. Risk assessment results
D. Current maturity level

**Answer: D**

## Question: 446

An IS auditor discovers that validation controls in a web application have been moved from the server side into the browser to boost performance. This would MOST likely increase the risk of a successful attack by:

A. phishing.
B. buffer overflow.
C. denial of service (DoS).
D. structured query language (SQL) injection.

**Answer: B**

## Question: 447

During a review of a production schedule, an IS auditor observes that a staff member is not complying with mandatory operational procedures-The auditor's NEXT step should be to:

A. issue an audit memorandum identifying the noncompliance.
B. determine why the procedures were not followed.
C. include the noncompliance in the audit report.
D. note the noncompliance in the audit working capers.

**Answer: C**

## Question: 448

The business owner's approval of software changes being moved into production is PRIMARILY necessary to:

A. prevent unauthorized access to data.
B. confirm there is a process to control system changes.
C. ensure that an application functionality requirement is satisfied.
D. inform management of deployments of new functionality.

**Answer: D**

## Question: 449

Which of the following provides for the GREATEST cost reduction in a large data center?

A. Power conditioning
B. Job-scheduling software
C. Server consolidation
D. Staff rotation

**Answer: C**

## Question: 450

Which of the following would be MOST important to update once a decision has been made to outsource a critical application to a cloud service provider?

A. IT budget
B. Business impact analysis (BIA)
C. IT resource plan
D. Project portfolio

**Answer: B**

## Question: 451

An IS auditor is reviewing a mobile app that allows customers to submit payments for bills. As part of the review, the auditor examines how code is developed and deployed to production. It is determined that a secure code review is done prior to each deployment to production. What type of control is being used?

A. Directive
B. Compensating
C. Preventive
D. Corrective

**Answer: C**

## Question: 452

Which of the following is the BEST approach to help ensure evidence from a computer forensics investigation is legally admissible?

A. The computer suspected of storing the evidence Is isolated, and the Incident response Mm is contacted for investigation.

B. The relevant data is extract from system, firewall and IDS logs then consolidated as evidence.
C. The media involved is preserved using imaging, and further analysis is performed on the image instead of The original.
D. The incident response team reviews and analyzes the evidence, and the evidence file is then securely deleted to avoid further damage.

**Answer: A**

## Question: 453

The BEST way for an IS auditor to determine which business processes are currently outsourced to a specific service provider is to review the:

A. request for proposal (RFP) responses.
B. service provider's contract.
C. enterprise architecture (EA) diagram.
D. vendor management policy.

**Answer: B**

## Question: 454

Which of the following is MOST important in the audit quality assurance process?

A. Results of corrective action plans
B. Qualifications of the assessor
C. Oversight by the audit committee
D. Testing performed during the assessment

**Answer: A**

## Question: 455

IS management has decided to replace the current single-server-based local area network (LAN) with three interconnected servers running different operating systems. Existing applications and data on the old server have been exclusively distributed on the new servers. This will MOST likely result in:

A. data incompleteness.
B. multiple authentication.
C. data unavailability,
D. disclosure of information.

**Answer: C**

## Question: 456

The decision to accept an IT control risk related to data quality should be the responsibility of the:

A. information security team.
B. chief information officer (CIO).
C. business owner.
D. IS audit manager.

**Answer: A**

## Question: 457

Which of the following is the MOST important reason for updating and retesting a business continuity plan (BCP)7

A. Staff turnover
B. Emerging technology
C. Matching industry best practices
D. Significant business change

**Answer: D**

## Question: 458

An IS auditor reviewing a production support team's incident management procedures is evaluating whether appropriate prioritization criteria have been defined. Which of the following is MOST important to include as part of the prioritization criteria?

A. Cost to restore
B. Time to repair
C. Restore point
D. Business impact

**Answer: D**

## Question: 459

Which of the following is the BEST way to minimize leakage of data in transit?

A. Digital signature
B. Virtual local area network (VLAN)
C. Virtual private network (VPN)
D. Storage encryption

**Answer: C**

## Question: 460

Previous audits have found that a large organization has had a number of segregation of duties conflicts between various roles, and the IT governance committee has asked the audit function for guidance on how to address this issue. Which of the following is the BEST recommendation?

A. Revise the user organizational structure and policies
B. Conduct a risk assessment and develop mitigating controls.
C. Review system access logs to identify escalation of user privileges.
D. Institute additional supervisory approvals when granting system access.

**Answer: B**

## Question: 461

An organization has recently converted its infrastructure to a virtualized environment. The GREATEST benefit related to disaster recovery is that virtualized servers:

A. eliminate the manpower necessary to restore the server.
B. decrease the recovery time objective (RTO).
C. reduce the time it takes to successfully create backups.
D. can be recreated on similar hardware faster than restoring from backups.

**Answer: B**

## Question: 462

Which of the following should be of GREATEST concern to an organization's board when reviewing the internal audit department's quality assurance and improvement program?

A. The program does not incorporate recommendations from prior audits.
B. The program has not been approved by senior management.
C. The program does not Include periodic external assessments.

D. Program metrics have not been updated in over two years.

**Answer: B**

## Question: 463

Which of the following indicates the HIGHEST level of maturity for an organization's information systems internal control environment?

A. Controls are regularly evaluated using a formally documented process.
B. Controls are adequately documented and control exceptions are captured.
C. The operation of controls depends on employee knowledge.
D. Operational effectiveness is evaluated upon management request

**Answer: A**

## Question: 464

An IS auditor was involved in the design phase for a new system's security architecture. For the planned post-implementation audit which of the following would be the MOST appropriate course of action for the auditor?

A. Have another auditor review the security architecture.
B. Disclose the independence Issues in the audit report.
C. Change the audit scope to exclude security architecture.
D. Postpone the post-implementation audit to a later date.

**Answer: A**

## Question: 465

During a follow-up audit, an IS auditor finds that some critical recommendations have not been addressed as management has decided to accept the risk. Which of the following is the IS auditor's BEST course of action?

A. Adjust the annual risk assessment accordingly.
B. Update the audit program based on management's acceptance of risk.
C. Evaluate senior managements acceptance of the risk.
D. Require the auditee to address the recommendations in full.

**Answer: A**

## Question: 466

Buffer overflow in an Internet environment is of particular concern to the IS auditor because it can:

A. corrupt databases during the build.
B. cause the loss of critical data during processing.
C. cause printers to lose some of the document text when printing
D. be used to obtain improper access to a system.

**Answer: D**

## Question: 467

Which of the following would MOST effectively minimize the risk of unauthorized online banking customer transactions due to phishing?

A. Clear audit trails
B. An intrusion prevention system OPS)
C. A customer awareness program
D. A strong authentication mechanism

**Answer: C**

## Question: 468

An IT service desk has recorded several incidents related to server downtime following the failure of a network time protocol (NTP) server. Which of the following is the BEST methodology to help identify the root cause?

A. Crow-functional diagram
B. Data flow diagram
C. Server architecture diagram
D. Cause-and-effect diagram

**Answer: D**

## Question: 469

Which of the following BEST enables an IS auditor to identify gaps between the current state and future state of an organization's IT infrastructure?

A. Enterprise risk assessment
B. governance framework
C. Vulnerability assessment
D. Enterprise architecture

**Answer: D**

## Question: 470

Which of the following MOST efficiently protects computer equipment against short-term reductions in electrical power?

A. Surge protection devices
B. Alternative power supplies
C. Power line conditioners
D. Generators

**Answer: C**

## Question: 471

An organization has implemented application whitelisting in response to the discovery of a large amount of unapproved software. Which type of control has been deployed?

A. Preventive
B. Directive
C. Detective
D. Corrective

**Answer: B**

## Question: 472

When designing a data analytics process, which of the following should be the stakeholder's role in automating data extraction and validation?

A. Allocating the resources necessary to purchase the appropriate software packages
B. Performing the business case analysis for the data analytics initiative

C. Indicating which data elements are necessary to make informed decisions
D. Designing the workflow necessary for the data analytics tool to evaluate the appropriate data

**Answer: D**

## Question: 473

An organization recently implemented an industry-recognized IT framework to improve the overall effectiveness of IT governance. Which of the following would BEST enable an IS auditor to assess the implementation against the framework?

A. Balanced scorecard
B. Key risk Indicators (KRIs)
C. Industry benchmarking
D. Capability maturity model

**Answer: D**

## Question: 474

In a RAO model, which of the following roles must be assigned to only one individual?

A. Accountable
B. Consulted
C. informed
D. Responsible

**Answer: A**

## Question: 475

Which of the following controls MOST effectively reduces the risk associated with use of instant messaging (IM) in the workplace?

A. Network address translation
B. Traffic encryption
C. Session border controllers
D. Blocking peer-to-peer (P2P) clients

**Answer: B**

## Question: 476

Which of the following would MOST effectively detect a condition where an employee assigned to an operations role could perform system administrator functions?

A. System review
B. Entitlement design review
C. User Access review
D. Business process review

**Answer: C**

## Question: 477

Which of the following is the MOST efficient solution for a multi-location healthcare organization that wants to be able to access patient data wherever patients present themselves for care?

A. Network segmentation
B. Dynamic localization
C. Software as a Service (SaaS) provider
D. Infrastructure as a Service (laaSJ provider

**Answer: B**

## Question: 478

Which of the following is the BEST way to detect potentially fraudulent purchases where an employee can approve a receipt of an item or service that the employee also procured?

A. Require trial invoices can only be paid when matched with purchase orders.
B. Require receipts to be entered against purchase orders by someone other than the buyer.
C. Require staff training on entering purchase orders into the enterprise resource planning (ERP) system.
D. Require purchase orders to originate from the same individual with designated authority.

**Answer: B**

## Question: 479

An IS auditor would be concerned if the quality assurance (QA) function were found to be performing which of the following roles?

A. Reviewing the code to ensure proper documentation and development practices were followed
B. Submitting corrected code for issues identified through the testing process
C. Ensuring the development methods and standards are adhered to throughout the process
D. Evaluating whether the testing assumptions and developed code are aligned to the design criteria

**Answer: B**

## Question: 480

Which of the following BEST provides audit management with a view of potential performance improvements within the organizations IS audit function?

A. Quality management policies
B. Auditor independence checklists
C. Auditor performance reviews
D. Post-audit quality reviews

**Answer: D**

## Question: 481

Which of the following is MOST helpful when establishing the authenticity of digital evidence collected from a hard disk?

A. Mash of the files on the hard disk
B. Confirmation by witnesses
C. Chain of custody documentation
D. Bit-by-bit image of the hard disk

**Answer: D**

## Question: 482

Which of the following poses the GREATEST risk to the enforceability of networking policies in a virtualized environment?

A. Use of 3 public key infrastructure
B. Lack of encryption for data at rest
C. Transmission of data on public networks
D. Lack of visibility into the networks

**Answer: D**

## Question: 483

An IS auditor finds ad hoc vulnerability scanning is in place with no clear alignment to the organization's wider security threat and vulnerability management program. Which of the following would BEST enable the organization to work toward improvement in this area?

A. Maintaining a catalog of vulnerability that may impact mission-critical systems
B. Outsourcing the threat and vulnerability management function to a third party
C. Using a capability maturity model to identify a path to an optimized program
D. Implementing security logging to enhance threat and vulnerability management

**Answer: A**

## Question: 484

An IS auditor discovers that management has created a system interface to receive financial data and store it in a data warehouse. Which of the following provides the BEST assurance that data in the data warehouse is accurate?

A. Established risk management processes
B. A documented change management process
C. Management, access reviews
D. Management reconciliations

**Answer: D**

## Question: 485

Which of the following should an IS auditor use when verifying a three-way match has occurred in an enterprise resource planning (ERP) system?

A. Purchase requisition
B. Goods delivery notification
C. Purchase order
D. Bank confirmation

**Answer: D**

## Question: 486

Which of the following BEST facilitates the ability to efficiently allocate time, effort, and resources to address security incidents?

A. Incident escalation
B. Incident monitoring
C. Incident definition
E. Incident classification

**Answer: D**

## Question: 487

An organization plans to allow third parties to collect customer personal data from a retail loyalty platform via an application programming interface (API). Which of the following should be the PRIMARY consideration when designing this API?

A. Data governance polices
B. System resilience
C. Data availability
D. Regulatory compliance

**Answer: D**

## Question: 488

An IS auditor is using data analytics for an accounts payable audit. Which of the following potential risk scenarios will MOST likely be identified using this approach?

A. Consecutive invoice numbers paid
B. Duplicate payments made for a vendor
C. Rogue or shadow vendors
D. Payments made to the wrong vendor

**Answer: B**

## Question: 489

Of the following, who should authorize a project management team's request to take a mission-critical application offline to implement a new release and configuration?

A. Chief information security officer (CISO)
B. Project manager
C. Business process owner
D. Application administrator

**Answer: C**

## Question: 490

An IS auditor performing an application development review attends development team meetings. The IS auditor's independence will be compromised if the IS auditor:

A. designs and executes the user's acceptance test plan.
B. assists in developing an integrated test facility on the system.
C. reviews the result of systems tests that were performed by the development team.
D. re-performs test procedures used by the development team.

**Answer: A**

## Question: 491

Which of the following BEST enables an audit department to improve the quality of work performed by its auditors?

A. Using audit-related data analytics tools
B. funding additional resources for audit work
C. Implementing global quality standards
D. Implementing peer review of audit work

**Answer: A**

## Question: 492

Which of the following is MOST important for an organization to review before sharing data with an external business partner via an application programming interface (API)?

A. The business partner's help desk incident tickets
B. The business partner's web application log files
C. The business partner's security practices

D. The business partner's data center access logs

**Answer: B**

## Question: 493

Prior to the migration of acquired software into production, it is MOST important that the IS auditor review the:

A. system documentation.
B. vendor testing report.
C. user acceptance lest report.
D. source code escrow agreement.

**Answer: A**

## Question: 494

An IS auditor reviewing a recently implemented virtual environment notices discrepancies among similar machine setups. Which of the following should the auditor recommend to minimize configuration risks?

A. Implement templates to manage rapid deployment of virtual machines.
B. Implement network best practice recommendations.
C. Perform hypervisor software updates with available patches to minimize security weaknesses.
D. Perform architectural vulnerability analysis to compare current system attributes to a

**Answer: A**

## Question: 495

A new regulatory standard for data privacy requires an organization to protect personally identifiable information (Pll). Which of the following is MOST important to include in the audit engagement plan to assess compliance with the new standard?

A. Review of data protection procedures
B. Review of data loss risk scenarios
C. Identification of IT systems that host Pll
D. Certification of unencrypted Pll

**Answer: A**

## Question: 496

In attribute sampling, what is the relationship between expected error rate and sample size?

A. The greater the expected error rate. The greater the sample size.
B. The greater the expected error rate, the smaller the sample size.
C. The greater the sample size, the tower The expected error rate.
D. The sample size is not affected by expected error rate.

**Answer: B**

## Question: 497

Which of the following is the MOST effective way for an IS auditor to identify unauthorized changes to the production state of a critical business application?

A. Review recent updates in the configuration management database (CMDB) for compliance with IT patches.
B. Run an automated scan of the production environment to detect missing software patches.
C. Compare a list of production system changes with the configuration management database
D. Review recently approved changes to application programming interfaces (API) in the production environment.

**Answer: C**

## Question: 498

Which of the following is the Most effective method to address software license violations on employee workstations?

A. Restricting administrative rights on employee workstations
B. Requiring automated installation of software
C. Scanning of workstations daily for unauthorized software use
D. Implementing real-time monitoring software on employee workstations

**Answer: A**

## Question: 499

Which of the following is the MOST important reason to classify a disaster recovery plan (DRP) as confidential?

A. Comply with business continuity best practice.
B. Protect the plan from unauthorized alteration.
C. Ensure compliance with the data classification policy.
D. Reduce the risk of data leakage that could lead to an attack.

**Answer: C**

## Question: 500

Which of the following would provide management with the MOST reasonable assurance that a new data warehouse will meet the needs of the organization?

A. Integrating data requirements into the system development life cycle (SDLC)
B. Appointing data stewards to provide effective data governance
C. Facilitating effective communication between management and developers
D. Classifying data quality issues by the severity of their impact to the organization

**Answer: C**

## Question: 501

Which of the following tests would provide the BEST assurance that a health care organization is handling patient data appropriately?

A. Compliance with action plans resulting from recent audits
B. Compliance with industry standards and best practice
C. Compliance with local laws and regulations
D. Compliance with the organization's policies and procedures

**Answer: A**

## Question: 502

Which of the following is the MOST important consideration when establishing vulnerability scanning on critical IT infrastructure?

A. The scanning will be performed during non-peak hours.
B. The scanning will be cost-effective.
C. The scanning will be followed by penetration testing.

D. The scanning will not degrade system performance.

**Answer: C**

## Question: 503

A security review focused on data loss prevention (DLP) revealed the organization has no visibility to data stored in the cloud. What is the IS auditors BEST recommendation to address this issue?

A. Employ a cloud access security broker (CASB).
B. Enhance the firewall at the network perimeter.
C. Utilize a DLP tool on desktops to monitor user activities.
D. Implement a file system scanner to discover data stored in the cloud.

**Answer: B**

## Question: 504

Which of the following is the PRIMARY responsibility of an organization's IT steering committee?

A. Conducting peer reviews of other organizations
B. Identifying new technological threats
C. Reporting on key performance measures
D. Communicating strategic goals to IT project teams

**Answer: D**

## Question: 505

Which of the following is the BEST way to ensure enterprise architectural objectives are aligned with business and technology objectives?

A. Identify dependencies between current and future state technologies.
B. Adopt industry-approved architecture standards and best practices.
C. Optimize technology investments with business requirements.
D. Identify business stakeholder responsibilities for IT projects.

**Answer: C**

## Question: 506

When auditing the effectiveness of a biometric system, which of the following indicators would be MOST important to review?

A. Failure to enroll rate
B. System response time
C. False acceptance rate
D. False negatives

**Answer: C**

## Question: 507

When reviewing user access to an application containing sensitive company data, which of the following should be the GREATEST concern with regard to segregation of duties?

A. The database administrator performs system analyst functions.
B. The network administrator performs security administrator functions.
C. The application programmer performs quality assurance functions.
D. The help desk performs application backups.

**Answer: A**

## Question: 508

Communicating which of the following would BEST encourage management to initiate appropriate actions following the receipt of report findings?

A. Statistical sampling used to derive observations
B. Risk implications of the observations
C. Strict deadlines to close all observations
D. Recommendations that align with the business strategy

**Answer: D**

## Question: 509

The PRIMARY purpose of an internal audit department's quality assurance improvement program is to evaluate which of the following?

A. The efficiency of internal audit processes
B. The adequacy and qualifications of internal audit personnel

C. The accuracy of prior-year internal audit results
D. The effectiveness of the internal audit function

**Answer: D**

## Question: 510

Total billing amounts on invoices are automatically transferred to an organization's account ledger weekly. During an IS audit, the auditor discovers that one week's billing is missing from the ledger. Which of the following areas should the auditor examine FIRST?

A. Module access rights
B. Batch processing controls
C. Change management
D. Annual reconciliations

**Answer: B**

## Question: 511

A financial institution suspects that a manager has been crediting customer accounts without authorization. Which of the following is the MOST effective method to validate this concern?

A. Variable sampling
B. Attribute sampling
C. Stop or go sampling
D. Discovery sampling

**Answer: B**

## Question: 512

As part of a post-implementation review, the BEST way to assess the realization of outcomes is by:

A. obtaining feedback from the user community.
B. evaluating the actual performance of the system.
C. performing a comprehensive risk analysis.
D. comparing the business case benefits to the achieved benefits.

**Answer: D**

## Question: 513

Using swipe cards to limit employee access to restricted areas requires implementing which additional control?

A. Periodic review of access profiles by management
B. Physical sign-in of all employees for access to restricted areas
C. Initial escort of all new hires by a current employee
D. Employee-access criteria determined on the basis of IS experience

**Answer: C**

## Question: 514

Which of the following should occur EARLIEST in a business continuity management lifecycle?

A. Defining business continuity procedures
B. Carrying out a threat and risk assessment
C. Developing a training and awareness program
D. Identifying critical business processes

**Answer: D**

## Question: 515

What is the purpose of using a write blocker during the acquisition phase of a digital forensics investigation?

A. To prevent the actuation of installed malware
B. To protect against self-destruct utilities
C. To preserve chain of custody
D. To prevent evidence alteration

**Answer: D**

## Question: 516

organization has outsourced some of its subprocesses to a service provider. When scoping the audit of the provider, the organization's internal auditor should FIRST

A. discuss audit objectives with the provider.
B. review internal audit reports of the provider.
C. review the contract with the provider.
D. evaluate operational controls of the provider.

**Answer: C**

## Question: 517

Which of the following is the MOST appropriate document for granting authority to an external IS auditor in an audit engagement with a client organization?

A. Approved statement of work
B. Formally approved audit charter
C. An internal memo to all concerned parties
D. Request for proposal for audit services

**Answer: A**

## Question: 518

An IS auditor wants to determine who has oversight of staff performing a specific task and is referencing the organization's RAG chart. Which of the following roles within the chart would provide this information?

A. Consulted
B. Responsible
C. Accountable
D. Informed

**Answer: C**

## Question: 519

The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

A. nonrepudiation.
B. integrity.
C. authorization.
D. authenticity.

**Answer: C**

## Question: 520

Which of the following findings would be of MOST concern to an IS auditor performing a review of an end-user developed application that generates financial statements?

A. There is no adequate user license for the application.
B. There is not adequate training in the use of the application.
C. There is no control to ensure accuracy of the processed data.
D. The application is not sufficiently supported by the IT department

**Answer: C**

## Question: 521

Which of the following is the MOST important consideration when developing an incident response program?

A. Number of dedicated response staff
B. Technical skills of response staff
C. Senior management support
D. Incident response procedures

**Answer: C**

## Question: 522

Which of the following auditing techniques would be used to detect the validity of a credit card transaction based on time, location, and date of purchase?

A. Data mining
B. Stratified sampling
C. Benford's analysis
D. Gap analysis

**Answer: B**

## Question: 523

A new regulation in one country of a global organization has recently prohibited cross-border transfer of personal dat
a. An IS auditor has been asked to determine the organization's level of exposure in the affected country. Which of the following would be MOST helpful in making this assessment?
A. Identifying data security threats in the affected jurisdiction
B. Identifying business processes associated with personal data exchange with the affected jurisdiction
C. Reviewing data classification procedures associated with the affected jurisdiction
D. Developing an inventory of all business entities that exchange personal data with the affected jurisdiction

**Answer: B**

## Question: 524

What is an IS auditor's BEST course of action when provided with a status update indicating audit recommendations related to segregation of duties for financial staff have been implemented?

A. Verify sufficient segregation of duties controls are in place.
B. Request documentation of the segregation of duties policy and procedures.
C. Note the department's response in the audit workpapers and records.
D. Confirm with the business that the recommendations are implemented.

**Answer: A**

## Question: 525

To BEST determine if a project is successfully addressing business requirements while managing the associated risk, which of the following should an IS auditor expect to find at each significant milestone?

A. Post-implementation review with affected parties
B. A revised business impact and risk analysis
C. Formal acceptance by appropriate stakeholders
D. Comprehensive end user acceptance testing

**Answer: C**

## Question: 526

An information systems security officer's PRIMARY responsibility for business process applications is to:

A. create role-based rules for each business process.
B. authorize secured emergency access.

C. approve the organization's security policy.
D. ensure access rules agree with policies.

**Answer: D**

## Question: 527

Which of the following is the BEST way to reduce the risk of vulnerabilities during the rapid deployment of container-based applications to a hybrid cloud?

A. Conduct security auditing during the development life cycle.
B. Review a sample of historical production changes to identify abnormalities.
C. Review development and operations (DevOps) policies and procedures.
D. Conduct a post-deployment security audit to identify vulnerabilities.

**Answer: C**

## Question: 528

Which of the following testing approaches provides the GREATEST assurance that only approved systems development releases have been implemented in the production environment?

A. Test whether a sample of releases followed the organization's segregation of duties access controls.
B. Test whether a sample of developments in the systems development register have documented approvals.
C. Test whether a sample of releases in production migration logs have corresponding approvals.
D. Test whether a sample of approved developments have releases in production migration logs.

**Answer: C**

## Question: 529

Which of the following BEST supports an organization's planning efforts for investments in IT initiatives?

A. Continuous gap assessment
B. Enterprise architecture
C. Agile project management
D. Capability maturity model

**Answer: B**

## Question: 530

Incorporating the results of a maturity model assessment is MOST useful in the development of:

A. balanced scorecards.
B. key performance indicators (KPis).
C. key risk indicators (KRIs).
D. strategic implementation plans.

**Answer: A**

## Question: 531

Which of the following is MOST likely to improve the portability of an application connected to a database?

A. Using a structured query language (SQL)
B. Verifying database import and export procedures
C. Analyzing stored procedures and triggers
D. Optimizing the database physical schema

**Answer: A**

## Question: 532

Which of the following is the GREATEST risk associated with instant messaging?

A. Data classification procedures may not be followed.
B. Data governance may become ineffective.
C. Data logging is more difficult.
D. Data exfiltration is more likely to occur.

**Answer: D**

## Question: 533

In a small organization, an IS auditor finds that security administration and system analysis functions are performed by the same employee. Which of the following is the MOST significant finding?

A. The employee has not signed the security policy.

B. The employee's activities are not independently reviewed.
C. The security policy has not been updated to reflect the situation.
D. The employee's formal job description has not been updated.

**Answer: B**

## Question: 534

Which of the following is the BEST reason to utilize blockchain technology to record accounting transactions?

A. Integrity of records
B. Confidentiality of records
C. Availability of records
D. Distribution of records

**Answer: A**

## Question: 535

Which of the following is MOST important for an IS auditor to understand when planning an IS audit?

A. Inherent risk of auditable areas
B. Management focus on particular operations
C. Number of high-risk auditable processes
D. Availability of IS audit resources

**Answer: B**

## Question: 536

When reviewing an organization's data protection practices, an IS auditor should be MOST concerned with a lack of:

A. a security team.
B. data classification.
C. training manuals.
D. data encryption.

**Answer: B**

## Question: 537

When initiating an IT project, which of the following should be completed FIRST:'

A. Requirements definition
B. Project plan
C. Request for proposal
D. Feasibility study

**Answer: A**

## Question: 538

Which of the following is the BEST way for an IT forensics investigator to detect evidence of steganography?

A. Identify and analyze emergent properties within a file system's metadata.
B. Compare file hashes between original and modified image files.
C. Recover deleted files from a suspected hard drive utilizing forensics software.
D. Scan computer operating systems using administrative tools.

**Answer: B**

## Question: 539

An IS auditor is reviewing an organization's implementation of a bring your own device (BYOD) program. Which of the following would be the BEST recommendation to help ensure sensitive data is protected if a device is in the possession of an unauthorized individual?

A. Enable the location service feature on devices.
B. Encrypt data on devices including storage media.
C. Authenticate device users when accessing the corporate network.
D. Enable remote wiping of critical data.

**Answer: B**

## Question: 540

Which of the following is the BEST control to protect an organization's sensitive data when using a publicly available cloud storage service?

A. Transparent volume encryption offered by the cloud vendor
B. Data encryption performed by the organization prior to uploading
C. Transport layer security (TLS) between the cloud vendor and the organization
D. Cryptographic hash function performed by the cloud vendor

**Answer: B**

## Question: 541

Which of the following activities should an IS auditor perform FIRST during an external network security assessment?

A. Enumeration
B. Reconnaissance
C. Exploitation
D. Vulnerability scanning

**Answer: A**

## Question: 542

Which of the following is the BEST evidence that an organization is aware of applicable laws and regulations?

A. The organization's compliance matrix
B. History of legal actions and regulatory correspondence
C. The existence of an employee awareness training program
D. Industry benchmark results

**Answer: A**

## Question: 543

A manufacturing company is implementing application software for its sales and distribution system. Which of the following is the MOST important reason for the company to choose a centralized online database?

A. Elimination of multiple points of failure
B. Elimination of the need for data normalization
C. Enhanced data redundancy
D. Enhanced integrity controls

**Answer: D**

## Question: 544

Which of the following would be the MOST effective method for detecting duplicate payments?

A. Reviewing sequence numbers and time stamps for each transaction
B. Using a cryptographic hashing algorithm
C. Enciphering and deciphering the message digest
D. Assessing payment history for reasonableness and approval

**Answer: A**

## Question: 545

Which of the following is MOST important to consider when reviewing a third-party service agreement for disaster recovery services'

A. Provisions exist to retain ownership of intellectual property in the event of termination,
B. Security and regulatory requirements are addressed in the agreement.
C. The lowest price possible is obtained for the service rendered.
D. Recovery point objectives (RPOs) and recovery time objectives (RTOs) are included in the agreement.

**Answer: A**

## Question: 546

When developing metrics to measure the contribution of IT to the achievement of business goals, the MOST

A. are used by similar industries to measure the effect of IT on business strategy.
B. measure the effectiveness of IT controls in the achievement of IT strategy.
C. provide quantitative measurement of IT initiatives in relation with business targets,
D. are expressed in terms of how IT risk impacts the achievement of business goals.

**Answer: C**

## Question: 547

An IS auditor is reviewing an organization's method to transport sensitive data between offices. Which of the following would cause the auditor MOST concern?

A. The method relies exclusively on the use of asymmetric encryption algorithms.
B. The method relies exclusively on the use of symmetric encryption algorithms.
C. The method relies exclusively on the use of public key infrastructure.
D. The method relies exclusively on the use of digital signatures.

**Answer: B**

## Question: 548

Audit software designed to detect invalid data, extreme values, or linear correlations between data elements can be classified as which type of data analytics tool?

A. Descriptive
B. Prescriptive
C. Diagnostic
D. Predictive

**Answer: C**

## Question: 549

The BEST way to assure an organization's board of directors that IT strategies support business objectives is to:

A. identify and repent on the achievement of critical success factors (CSFs).
B. ensure that senior business managers review IT budgets.
C. provide regular assessments of emerging technologies.
D. confirm that IT strategies have been fully documented and disseminated.

**Answer: A**

## Question: 550

Which of the following would be an INAPPROPRIATE activity for a network administrator?

A. Analyzing network security incidents
B. Prioritizing traffic between subnets
C. Modifying a router configuration
D. Modifying router log files

**Answer: D**

## Question: 551

Which of the following is the BEST recommendation for the establishment of an information security policy?

A. The policy and guidelines should b« developed by the human resources department.
B. The policy should be developed by the security administrator.
C. The development and approval should be overseen by business area management.
D. The policy should be developed by IS management

**Answer: C**

## Question: 552

When using a wireless device, which of the following BEST ensures confidential access to email via web mail?

A. Wired equivalent privacy (WEP)
B. Hypertext transfer protocol secure (HTTPS)
C. Simple object access protocol (SOAP)
D. Extensible markup language (XML)

**Answer: B**

## Question: 553

IT help desk statistics show a high number of recurring incidents with known solutions. Which of the following is the BEST IS audit recommendation?

A. Outsource the IT help desk.
B. Provide better training to end users.
C. Implement incident escalation
D. Hire additional technical support staff.

**Answer: B**

## Question: 554

Which of the following should be of GREATEST concern when conducting an audit of software inventory management?

A. Development libraries not included in inventory records
B. Anti-virus software not regularly upgraded
C. Missing licensing paper contracts
D. Unlicensed software

**Answer: D**

## Question: 555

What is the MOST difficult aspect of access control in a multiplatfotm, multiple-site client/server environment?

A. Restricting a local user to necessary resources on a local platform
B. Maintaining consistency throughout all platforms
C. Restricting a local user to necessary resources on the host server
D. Creating new user IDs valid only on a few hosts

**Answer: B**

## Question: 556

An audit of a database management system found the audit log was not restarted following maintenance. Which of the following is the GREATEST concern to the IS auditor?

A. The database triggers and pointers will not be optimized.
B. The database optimization will be compromised.
C. Changes by the database administrators will not be logged.
D. Changes by application users will not be logged.

**Answer: C**

## Question: 557

An IS auditor observed that most users do not comply with physical access controls. The business manager has explained that the control design is inefficient. What is the auditor's BEST course of action?

A. Work with management to design and implement a better control.
B. Identify the impact of control failure and report the finding with a risk rating.

C. Recommend changing the access control process to increase efficiency.
D. Redesign and retest the physical access control.

**Answer: B**

## Question: 558

To protect information assets, which of the following should be done FIRST?

A. Encrypt data.
B. Restrict access to data.
C. Back up data.
D. Classify data.

**Answer: D**

## Question: 559

Which of the following should an IS auditor review FIRST when evaluating incident management procedures?

A. Command center monitoring
B. Prioritization criteria Peer
C. review requirements
D. Root cause analysis steps

**Answer: B**

## Question: 560

Which of the following controls can BEST detect accidental corruption during transmission of data across a network?

A. Parity checking
B. Sequence checking
C. Check digit verification
D. Symmetric encryption

**Answer: B**

## Question: 561

For a company that outsources payroll processing, which of the following is the BEST way to ensure that only authorized employees are paid?

A. Only payroll employees should be given the password for data entry and report retrieval.
B. Employees should receive pay statements showing gross pay, net pay. and deductions.
C. The company's bank reconciliations should be independently prepared and checked.
D. Electronic payroll reports should be independently reviewed.

**Answer: C**

## Question: 562

Which of the following presents the GREATEST security risk to an organization using peer-to-peer (P2P) file-sharing networks?

A. Penetration testing cannot identify issues with P2P file-sharing networks.
B. Controls are difficult to apply to unstructured networks.
C. There is no audit trail for files residing outside of the organization.
D. IP addresses are shared to create a connection.

**Answer: B**

## Question: 563

An audit group is conducting a risk assessment as part of a risk-based audit strategy. To help ensure the risk assessment results are relevant to the organization, it is MOST important to:

A. include operational departments and processes.
B. determine both the inherent risk and detection risk.
C. understand the organization's controls.
D. understand the organization's objectives and risk appetite.

**Answer: D**

## Question: 564

The performance of an order-processing system can be measured MOST reliably by monitoring:

A. heartbeats between server systems.
B. application and database servers' CPU load.
C. turnaround time of completed transactions.
D. input/request queue length.

**Answer: C**

## Question: 565

Which of the following should be an IS auditor's PRIMARY concern when evaluating an organization's information security policies, procedures, and controls for third-party vendors?

A. The organization is still responsible for protecting the data.
B. The same procedures and controls are used for all third-party vendors.
C. The third-party vendors have their own information security requirements.
D. Noncompliance is easily detected.

**Answer: C**

## Question: 566

Which of the following should be of GREATEST concern to an IS auditor reviewing an organization's initiative to adopt an enterprise governance framework?

A. The organization has not provided employees with formal training on the framework.
B. The organization's security department has not been involved with the initiative.
C. The organization has tried to adopt the entire framework at once.
D. The organization has not identified the business drivers for adopting the framework.

**Answer: D**

## Question: 567

Which of the following would BEST determine whether a post-implementation review (PIR) performed by the project management office (PMO) was effective?

A. The review was performed by an external provider.
B. Project outcomes have been realized.
C. Management approved the PIR report.
D. Lessons learned were implemented.

**Answer: B**

## Question: 568

In an organization that has a staff-rotation policy, the MOST appropriate access control model is:

A. discretionary.
B. lattice-based.
C. mandatory.
D. role-based.

**Answer: D**

## Question: 569

When reviewing a contract for a disaster recovery hot site, which of the following would be the MOST significant omission?

A. Equipment provided
B. Testing procedures
C. Audit rights
D. Exposure coverage

**Answer: D**

## Question: 570

An accounts receivable data entry routine prevents the entry of the same customer with different account numbers. Which of the following is the BEST way to test if this programmed control is effective?

A. Implement a computer-assisted audit technique (CAAT).
B. Compare source code against authorized software.
C. Review a sorted customer list for duplicates.
D. Attempt to create a duplicate customer.

**Answer: D**

## Question: 571

During a follow-up audit for a finding related to change management, an IS auditor notes that one of the changes sampled was an emergency change, which follows a different process. Which of the following is the auditor's BEST course of action?

A. Select a replacement change for testing.
B. Obtain evidence that the change was approved.
C. Mark the sample as not applicable in the workpaper and move on to testing the next sample.
D. Note the sample as a deviation and leave the finding open in the audit tracking log.

**Answer: B**

## Question: 572

Which of the following access fights presents the GREATEST risk when granted to a new member of the system development staff?

A. Write access to development data libraries
B. Write access to production program libraries
C. Execute access to development program libraries
D. Execute access to production program libraries

**Answer: B**

## Question: 573

A database is denormalized in order to:

A. prevent loss of data.
B. save storage space.
C. increase processing efficiency.
D. ensure data integrity.

**Answer: C**

## Question: 574

The final acceptance testing of a new application system should be the responsibility of the:

A. IS audit team.
B. user group.
C. IS management.
D. quality assurance team

**Answer: B**

## Question: 575

Which of the following sampling methods is the BEST approach for drawing conclusions based on frequency of occurrence?

A. Attribute sampling
B. Difference estimation sampling
C. Monetary estimation sampling
D. Stratified sampling

**Answer: A**

## Question: 576

As part of a mergers and acquisitions activity, an acquiring organization wants to consolidate data and systems from the organization being acquired into existing systems. To ensure the data is relevant the acquiring organization should:

A. define data quality requirements based on business needs.
B. implement a data warehouse solution.
C. automate the process of data collection and cleaning.
D. obtain data quality software.

**Answer: A**

## Question: 577

Which of the following should be a PRIMARY control objective when designing controls for system interfaces?

A. Ensure all data transferred through system interfaces is encrypted.
B. Ensure peer-to-peer data transfers are minimized.
C. Ensure managed file transfer (MFT) systems have restart capability for interruptions.
D. Ensure data on the sending system is identical to the data on the receiving system.

**Answer: A**

## Question: 578

An organization migrated most of its physical servers to virtual ones in its own data center. Which of the following should be of GREATEST concern to an IS auditor reviewing the virtual environment?

A. Virtual machine deployments are done without following an approved template.
B. Hypervisors have not been updated with the most recent patches.
C. Hypervisor access control lists are outdated.
D. The configuration management database (CMDB) does not include all virtual machines.

**Answer: A**

## Question: 579

Which function in the purchasing module of an enterprise resource planning (£RP) system ensures payments are not issued for incorrect invoices'

A. Sequential payment numbers
B. Management workflow approval
C. Three-way match
D. Purchasing authority levels

**Answer: C**

## Question: 580

Which of the following is the MOST significant obstacle to establishing a new privacy program?

A. A complex legal and regulatory landscape
B. Unresolved overlap of security and privacy roles and responsibilities
C. Failure to perform a business impact analysis (BIA)
D. An insufficient privacy awareness training program

**Answer: A**

## Question: 581

Which of the following factors constitutes a strength in regard to the use of a disaster recovery planning reciprocal agreement?

A. Reciprocal agreements may not be formally established in a contract.
B. The two companies might share a need for a specialized piece of equipment
C. Changes to the hardware or software environment by one company could make the agreement ineffective or obsolete.
D. A disaster could occur that would affect both companies.

**Answer: B**

## Question: 582

Which of the following is an indication of possible hacker activity involving voice communications?

A. A significant percentage of lines are busy during early morning and late afternoon hours.
B. Outbound calls are found to significantly increase in frequency during non-business hours.
C. Direct inward system access (OISA) is found to be disabled on the company's exchange.
D. Inbound calls experience significant fluctuations based on time-of-day and day-of-week.

**Answer: A**

## Question: 583

When developing a business continuity plan (BCP), which of the following steps should be completed FIRST?

A. Carry out a risk assessment.
B. Ensure that offsite backups can be efficiently restored.
C. Review the business continuity insurance policy.
D. Identify alternatives to critical applications.

**Answer: A**

## Question: 584

An operations manager has recently moved to internal audit Which of the following would be of GREATEST concern when assigning audit projects to this individual?

A. A control within the audit scope was implemented by the operations manager six months ago.
B. A control within the audit scope was downgraded to low risk by the operations manager six months ago.
C. The owner of a process within the audit scope worked for the operations manager six months ago.
D. A system within the audit scope is supported by an emerging technology for which the operations manager lacks experience.

**Answer: A**

## Question: 585

Which of the following stakeholders should be PRIMARILY responsible for developing, implementing, and monitoring metrics for security activities?

A. Chief information security officer
B. IT steering committee
C. Security incident response team
D. Chief technology officer

**Answer: A**

## Question: 586

An organization using instant messaging to communicate with customers prevent legitimate customers from being impersonated by:

A. Authentication users before conversation are initiated.
B. Using firewall to limit network traffic to authorized ports.
C. Logging conversation.
D. Using call monitoring.

**Answer: A**

## Question: 587

The MOST effective method for an IS auditor to determine which controls are functioning in an operating system is to:

A. Compare the current configuration to the corporate standard
B. Consult with the vendor of the system
C. Compare the current configuration to the default configuration
D. Consult with the systems programmer

**Answer: A**

## Question: 588

The CIO of an organization is concerned that the information security policies may not be comprehensive. Which of the following should an IS auditor recommend be performed FIRST?

A. Determine if there is j process to handle exceptions to the policies
B. Establish a governance board to track compliance with the policies
C. Obtain a copy of their competitor's policies
D. Compare the policies against an industry framework.

**Answer: D**

## Question: 589

The PRIMARY purpose for an IS auditor to review previous audit reports during the planning phase of a current audit is to:

A. identify applicable regulatory requirements for the current audit.
B. adjust audit scope to reduce testing in areas related to previous findings.
C. become informed about the auditee s business processes.
D. ensure that previously identified risks are addressed in the audit program.

**Answer: D**

## Question: 590

When physical destruction is not practical, which of the following is the MOST effective measure of disposing of sensitive data on a hard disk?

A. Deleting files sequentially
B. Overwriting multiple times
C. Recycling the disk
D. Reformatting

**Answer: C**

## Question: 591

A company has located its computer center on a moderate earthquake fault. Which of the following is the MOST important consideration in
establishing a contingency plan and an alternate processing site?

A. The alternative site does not reside on the same fault no matter how far the distance apart.

B. The alternative site is a hot site with equipment ready to resume processing immediately.
C. The contingency plan for high priority applications does not involve a shared cold site.
D. The contingency plan provides for backup tapes to be taken to the alternative site.

**Answer: A**

## Question: 592

During business process reengineering (BPR) of a bank's teller activities, an IS auditor should evaluate:

A. the impact of changed business processes.
B. the cost of new controls.
C. BPR project plans
D. continuous improvement and monitoring plans.

**Answer: A**

## Question: 593

Which of the following is the BEST indication of control maturity in an organization's systems development and implementation processes?

A. Code changes are tested and deployed manually.
B. Code changes are tested and deployed through automation.
C. Code changes are deployed to a test server and then to production.
D. Code changes are documented and approved.

**Answer: B**

## Question: 594

Which of the following firewall technologies involves examining the header of every packet of data traveling between the Internet and the corporate network without examining the previous packets?

A. Stateful filtering
B. Stateless filtering
C. Proxy servers
D. Bastion host

**Answer: B**

## Question: 595

An IS auditor is reviewing standards and compliance requirements related to an upcoming systems audit. The auditor notes that the industry
standards are less stringent than local regulatory standards. How should the auditor proceed?

A. Audit to the policies and procedures of the organization.
B. Coordinate with regulatory officers to determine necessary requirements.
C. Audit exclusively to the industry standards.
D. Audit to the standards with the highest requirements.

**Answer: D**

## Question: 596

Which of the following is MOST influential when defining disaster recovery strategies?

A. Annual loss expectancy
B. Maximum tolerable downtime
C. Data classification scheme
D. Existing server redundancies

**Answer: A**

## Question: 597

An audit report that specifies responsibility for the closure of noncompliance issues is BEST enhanced by including:

A. cost estimates for remediation.
B. a list of audit staff who will oversee remediation.
C. detailed mitigating steps.
D. target dates for remediation.

**Answer: C**

## Question: 598

Which of the following is the GREATEST advantage of implementing an IT enterprise architecture framework within an organization?

A. It reduces the overlap of infrastructure technologies within the organization.
B. It better equips an organization to adopt innovative and emerging technologies.
C. It helps to identify security issues in systems across the organization.
D. It improves the organization's ability to meet service level agreements (SLAs).

**Answer: D**

## Question: 599

Which of the following functions is MOST likely to be performed by an operating system utility residing on a web server?

A. Generating control totals for terminal devices such as point-of-sale devices
B. Configuring network protocols
C. Monitoring utilization activity and traffic patterns
D. Sending and receiving terminal warnings and error messages

**Answer: C**

## Question: 600

Which of the following is the GREATEST risk of cloud computing?

A. Lack of scalability
B. Reduced performance
C. Disclosure of data
D. Inflexibility

**Answer: C**

## Question: 601

An IS auditor s role in privacy and security is to:

A. implement risk management methodologies.
B. verify compliance with applicable laws.
C. assist in developing an IS security strategy.
D. assist the governance steering committee with implementing a security policy.

**Answer: B**

## Question: 602

An IS auditor suspects an organization's computer may have been used to commit a crime. Which of the following is the auditor s BEST course of
action?

A. Examine the computer to search for evidence supporting the suspicions.
B. Notify local law enforcement of the potential crime before further investigation.
C. Advise management of the crime after the investigation.
D. Contact the incident response team to conduct an investigation.

**Answer: D**

## Question: 603

Reviewing project plans and status reports throughout the development life cycle will:

A. facilitate the optimal use of resources over the life of the project.
B. eliminate the need to perform a risk assessment.
C. postpone documenting the project's progress until the final phase.
D. guarantee that the project will meet its intended deliverables.

**Answer: D**

## Question: 604

Which of the following would BEST help in classifying an organization s data?

A. Analysis of existing data handling procedures
B. Industry best practices for data classification
C. Impact of data loss or disclosure
D. Data retention requirements

**Answer: C**

## Question: 605

During the implementation of an upgraded enterprise resource planning (ERP) system, which of the following is the MOST important consideration foe a go-live decision?

A. Post-implementation review objectives
B. Test cases
C. Rollback strategy
D. Business case

**Answer: C**

## Question: 606

An IS auditor is reviewing the process followed in identifying and prioritizing the critical business processes. This process is part of the:

A. operations component of the business continuity plan (BCP).
B. enterprise risk management plan.
C. balanced scorecard.
D. business impact analysis (BIA).

**Answer: D**

## Question: 607

A digital signature addresses which of the following concerns?

A. Unauthorized reading
B. Message alteration
C. Message copying
D. Message theft

**Answer: B**

## Question: 608

An IS auditor is planning an audit of an organization s payroll processes. Which of the following is the BEST procedure to provide assurance
against internal fraud?

A. Compare employee work contracts against hours entered in the payroll system.
B. Interview the payroll manager to obtain a detailed process workflow.
C. Review management's approval of payroll system changes.
D. Review management's validation of payroll payment recipients.

**Answer: A**

## Question: 609

An organization has implemented a control to help ensure databases containing personal information will not be updated with online transactions that are incomplete due to connectivity issues. Which of the following information attributes is PRIMARILY addressed by this control?

A. Availability
B. Compliance
C. Confidentiality
D. integrity

**Answer: D**

## Question: 610

Which of the following could be determined by an entity-relationship diagram?

A. Links between data objects
B. How data are transformed at they move through the system
C. Modes of behavior of data objects
D. How the system behaves as a consequence of external events

**Answer: A**

## Question: 611

Which of the following is the BEST key performance indicator (KPI) for determining how well the IT policy is aligned to the business
requirements?

A. Number of inquiries regarding the policy
B. Total cost to support the policy
C. Number of approved exceptions to the policy
D. Total cost of policy breaches

**Answer: C**

## Question: 612

Which of the following is a benefit of requiring management to issue a report to stakeholders regarding the internal controls over IT?

A. Transparency of IT costs
B. Improved cost management
C. Improved portfolio management
D. Focus on IT governance

**Answer: D**

## Question: 613

While reviewing a hot site, the IS auditor discovers that one type of hardware platform is not installed. The IS auditor should FIRST

A. determine the business impact of the absence of the hardware.
B. establish the lead time for delivery of a new machine
C. recommend the purchase and installation of hardware at the hot site
D. report the finding immediately to senior IS management

**Answer: A**

## Question: 614

In which of the following cloud service models does the user organization have the GREATEST control over the accuracy of configuration items in
its configuration management database (CMDB)?

A. Software as a Service (SaaS)
B. Database as a Service (DbaaS)
C. Infrastructure as a Service (laaS)
D. Platform as a Service (PaaS)

**Answer: C**

## Question: 615

A start-up company acquiring for its order-taking system is unable to predict the volume of transactions. Which of the following is MOST important for the company to consider?

A. Configuration

B. Optimization
C. Compatibility
D. Scalability

**Answer: D**

## Question: 616

An IS auditor is assessing a recent migration of mission critical applications to a virtual platform. Which of the following observations poses the GREATEST risk to the organization?

A. The migration was not approved by the board of directors.
B. Training for staff with new virtualization responsibilities has not been conducted.
C. Role descriptions do not accurately reflect new virtualization responsibilities.
D. A post-implementation review of the hypervisor has not yet been conducted.

**Answer: C**

## Question: 617

Which of the following tools are MOST helpful for benchmarking an existing IT capability?

A. IT balanced scorecards
B. Risk assessments
C. IT maturity models
D. Prior IS audit reports

**Answer: C**

## Question: 618

Which of the following is MOST likely to be spoofed in an email transmission?

A. The path the message traveled through the Internet
B. The identity of the sending host
C. The identity of the receiving host
D. The identity of the sender

**Answer: D**

## Question: 619

Which of the following is the MAIN purpose of implementing an incident response process?

A. Assign roles and responsibilities
B. Comply with policies and procedures.
C. Provide substantial audit-trail evidence.
D. Manage impact due to breaches.

**Answer: D**

## Question: 620

When an intrusion into an organizations network is detected, which of the foflomng should be performed FIRST?

A. Identify nodes that have been compromised
B. Block all compromised network nodes
C. Develop a response to the incident
D. Protect information in the compromised systems

**Answer: D**

## Question: 621

An organization has outsourced its data processing function to a service provider. Which of the following would BEST determine whether the
service provider continues to meet the organization s objectives?

A. Periodic audits of controls by an independent auditor
B. Assessment of the personnel training processes of the provider
C. Adequacy of the service provider's insurance
D. Review of performance against service level agreements (SLAs)

**Answer: D**

## Question: 622

An internal audit has revealed a large number of incidents for which root cause analysis has not been performed. Which of the following is MOST

important for the IS auditor to verify to determine whether there is an audit issue?

A. Cost of resolving the incidents
B. Time required to resolve the incidents
C. Seventy level of the incidents
D. Frequency of the incidents

**Answer: C**

## Question: 623

Which of the following is the MOST effective control to restrict the use of instant messaging (IM) within an organization?

A. Application-based firewall
B. Antivirus software
C. Intrusion detection system (IDS)
D. Packet filtering firewall

**Answer: D**

## Question: 624

An IS auditor reviewing a new application for compliance with information privacy principles should be MOST concerned with:

A. collection limitation.
B. availability.
C. nonrepudiation.
D. awareness.

**Answer: A**

## Question: 625

When creating a new risk management program, it is CRITICAL to consider

A. the risk appetite.
B. risk mitigation techniques.
C. compliance measures.
D. resource utilization

**Answer: A**

## Question: 626

Which of the following would provide the BEST evidence for an IS auditor to determine whether segregation of duties is in place?

A. A walk-through of job functions
B. An analysis of user access requests
C. A review of the organizational chart
D. A review of personnel files

**Answer: B**

## Question: 627

Which of the following would help to ensure the completeness of batch file transfers?

A. Hash totals
B. Input controls
C. Self-checking digits
D. Parity check

**Answer: A**

## Question: 628

Which of the following is the safest means of transmitting confidential information over the Internet?

A. Establish a virtual private network (VPN) between the source and the destination.
B. Use asymmetric encryption and encrypt the data with a private key.
C. Send the data to a trusted third party to resend to the destination.
D. Break the data into many packets and send it over different routes.

**Answer: A**

## Question: 629

Which of the following would provide the BEST assurance that an organization s backup media is adequate in the case of a disaster?

A. Scheduled maintenance of the backup device
B. Scheduled read/write tests of the backup media
C. Regular review of backup logs to ensure that all data from the production environment is included
D. Regular recovery of production systems in a test environment

**Answer: D**

## Question: 630

Which of the following controls BEST mitigates the impact of a distributed denial of service (DDoS) attack against the controller in a softwaredefined network (SDN)?

A. Relocating virtualized network functions to physical infrastructure
B. Hardening the operating system that hosts the SDN controller
C. Implementing multiple physical SDN controllers
D. Implementing configuration management for SDN controllers

**Answer: B**

## Question: 631

An IS auditor is reviewing an organization's sales and purchasing system due to ongoing data quality issues. An analysis of which of the following would provide the MOST useful formation to determine the revenue loss?

A. Correlation between data errors and loss in value of transaction
B. Correlation between the number of issues and average downtime
C. Cost of implementing data validation controls within the system
D. Comparison of the cost of data acquisition and loss in sales revenue

**Answer: A**

## Question: 632

Which of the following should be the PRIMARY basis for planning and prioritizing IT infrastructure security audits?

A. Asset value to the organization
B. Management requests
C. The organization's risk appetite

D. Security best practice

**Answer: A**

## Question: 633

An IS Auditor is performing a business continuity plan (BCP) audit and identifies that the plan has not been tested for five years, however, the plan was successfully activated during a recent extended power outage. Which of the following is the 15 auditor's BEST count of action?

A. Determine if the annual BCP training program is in need of review
B. Determine if a follow-up BCP audit is required to identify future gaps
C. Determine if lessons learned from the activation were incorporated into the plan
D. Determine if the business impact analysis (BIA) is still accurate.

**Answer: C**

## Question: 634

An IS auditor has identified that some IT staff have administrative access to the enterprise resource planning (ERP) application, database, and
server. IT management has responded that due to limited resources, the same IT staff members have to support all three layers of the ERP
application. Which of the following would be the auditor's BEST recommendation to management?

A. Monitor activities of the associated IT staff members by reviewing system-generated logs weekly.
B. Request funding to hire additional IT staff to enable segregation of duties.
C. Remove some of the administrative access of the associated IT staff members.
D. Leverage business unit personnel to serve as administrators of the application.

**Answer: A**

## Question: 635

As part of a quality assurance initiative, an organization has engaged an external auditor to evaluate the internal IS audit function. Which of the
following observations should be of MOST concern?

A. The audit team is not sufficiently leveraging data analytics.
B. Audit reports are not approved by the audit committee.
C. Audit reports do not state they are conducted in accordance with industry standards.
D. Audit engagements are not risk-based.

**Answer: D**

## Question: 636

select a sample for testing, which must include the 80 largest client balances and a random sample of the rest, the IS auditor should recommend:

A. use of generalized audit software.
B. development of an integrated test facility (ITF).
C. applying attribute sampling using software.
D. sorting the file with a utility Release management

**Answer: C**

## Question: 637

What should be the PRIMARY basis for scheduling a follow-up audit?

A. The significance of reported findings
B. The completion of all corrective actions
C. The availability of audit resources
D. The time elapsed after audit report submission

**Answer: A**

## Question: 638

Which of the following is the MOST important consideration when developing an online business architecture and recovery strategy?

A. Single points of failure
B. Vendors network security
C. Immediate problem resolution
D. Vendors financial stability

**Answer: A**

## Question: 639

What should be an IS auditor s NEXT course of action when a review of an IT organizational structure reveals IT staff members have duties in
other departments?

A. Recommend that segregation of duties controls be implemented.
B. Report the issue to human resources (HR) management
C. Determine whether any segregation of duties conflicts exist.
D. Immediately report a potential finding to the audit committee.

**Answer: C**

## Question: 640

The MAJOR reason for replacing checks with electronic funds transfer (EFT) systems in the accounts payable area is to:

A. decrease the risk of unauthorized changes to payment transactions.
B. increase the efficiency of the payment process.
C. decrease the number of paper-based payment forms.
D. increase organizational credibility.

**Answer: B**

## Question: 641

An IS auditor should ensure that an application's audit trail:

A. has adequate security.
B. is accessible online.
C. does not impact operational efficiency
D. logs all database records.

**Answer: A**

## Question: 642

Which of the following would BEST assist senior management in evaluating IT performance as well as the alignment between corporate and IT strategic objectives?

A. Control self-assessment
B. IT project value analysis

C. Enterprise architecture
D. Balanced scorecard

**Answer: D**

## Question: 643

Which of the following is the GREATEST benefit of implementing an IT governance strategy within an organization?

A. IT projects are delivered on time and under budget
B. Management is aware of IT-related risks.
C. Employees understand roles and responsibilities
D. Reporting and metrics become higher priority.

**Answer: A**

## Question: 644

Which of the following would BEST provide executive management with current information on IT related costs and IT performance indicators?

A. Risk register
B. IT service management plan
C. Continuous audit reports
D. IT dashboard

**Answer: D**

## Question: 645

A web application is developed in-house by an organization. Which of the following would provide the BEST evidence to an IS auditor that the application is secure from external attack?

A. Code review by a third party
B. Web application firewall implementation
C. Penetration test results
D. Database application monitoring logs

**Answer: B**

## Question: 646

The PRIMARY objective of parallel testing an application is to confirm that:

A. the costs of running the new system are the same as running the old system.
B. new system processing times are similar to those of the old system.
C. system response times in the new system are better than the old system.
D. the results of calculations in the new system are as accurate as the old system.

**Answer: D**

## Question: 647

An IS auditor notes that due to the small size of the organization, human resources staff can create new employees in the payroll system as well
as process payroll. Which of the following is the BEST recommendation to address this situation?

A. Implement a periodic user access review over the payroll system.
B. Outsource the processing of payroll to a third party.
C. Hire additional staff so that access for the two functions can be segregated.
D. Implement periodic reviews of employees in the payroll system.

**Answer: A**

## Question: 648

When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs due to scope creep?

A. Change management
B. Problem management
C. Quality management
D. Risk management

**Answer: A**

## Question: 649

Which of the following is the PRIMARY responsibility of an organizations information security function?

A. Managing the organization's security procedures
B. Reviewing unauthorized attempts to access sensitive files
C. Approving access to data files
D. Installing network security programs

**Answer: A**

## Question: 650

As part of a follow-up of a previous year's audit, an IS auditor has increased the expected error rate for a sample. The impact will be:

A. required sample size increases.
B. sampling risk decreases.
C. degree of assurance increases.
D. standard deviation decreases.

**Answer: C**

## Question: 651

When an organization outsources a payroll system to a cloud service provider, the IS auditor's PRIMARY concern should be the:

A. service level agreement (SLA) is not reviewed annually.
B. service provider s platform is not compatible with legacy systems.
C. lack of independent assurance from a third party.
D. service provider s data center is on the ground floor.

**Answer: C**

## Question: 652

An IS auditor is evaluating the access controls at a multinational company with a shared network infrastructure. Which of the following is MOST
important?

A. Simplicity of end-to-end communication paths
B. Common security policies
C. Remote network administration
D. Logging of network information at user level

**Answer: B**

## Question: 653

Which of the following would BEST facilitate the successful implementation of an [T-related framework?

A. Involving appropriate business representation within the framework
B. Documenting IT-related policies and procedures
C. Aligning the framework to industry best practices
D. Establishing committees to support and oversee framework activities

**Answer: A**

## Question: 654

Which of the following is the BEST sampling method to use when estimating the rate of occurrence of a specific quality in a population?

A. Statistical sampling
B. Discovery sampling
C. Stop-or-go sampling
D. Attribute sampling

**Answer: D**

## Question: 655

The BEST data backup strategy for mobile users is to:

A. have them regularly back up data directories onto CD and courier the backups to the head office.
B. synchronize data directories automatically over the network.
C. mirror all data to a portable storage device.
D. have them regularly go to branch offices to perform backups.

**Answer: B**

## Question: 656

Which of the following is the BEST way to increase the effectiveness of security incident detection?

A. Determining containment activities based on the type of incident
B. Documenting root cause analysis procedures
C. Educating end users on identifying suspicious activity
D. Establishing service level agreements (SLAs) with appropriate forensic service providers

**Answer: C**

## Question: 657

What is the FIRST step an auditor should take when beginning a follow-up audit?

A. Review workpapers from the previous audit
B. Review previous findings and action plans
C. Meet with the auditee to discuss remediation progress
D. Gather evidence of remediation to conduct tests of controls

**Answer: B**

## Question: 658

An organization's current end-user computing practices include the use of a spreadsheet for financial statements. Which of the following is the GREATEST concern?

A. Operational procedures have not been reviewed in the current fiscal year
B. The spreadsheet is not maintained by IT.
C. The spreadsheet contains numerous macros.
D. Formulas are not protected against unintended changes.

**Answer: D**

## Question: 659

An organization uses electronic funds transfer (EFT) to pay its vendors. Which of the following should be an IS auditor s MAIN focus while reviewing controls in the accounts payable Application?

A. Amount of disbursements
B. Volume of transactions
C. Changes to the vendor master file
D. Frequency of transactions

**Answer: C**

## Question: 660

Which of the following test approaches would utilize data analytics to validate customer authentication controls for banking transactions?

A. Evaluate configuration settings for transactions requiring customer identification.
B. Review the business requirements document for customer identification requirements.
C. Review transactions completed for one period that have blank customer identification fields.
D. Attempt to complete a monetary transaction and leave the customer identification fields blank.

**Answer: C**

## Question: 661

The MAIN objective of incident management is to:

A. test for readiness to respond when facing an incident.
B. permit the incident to go on and follow the trail back to the beginning.
C. have an external computer security incident response team assess damage.
D. keep the business going while the response is occurring.

**Answer: D**

## Question: 662

Which of the following is the BEST method to assess the adequacy of security awareness in an organization?

A. Confirming a security awareness program exists
B. Interviewing employees about security responsibility
C. Administering security survey questionnaires
D. Observing employee security behaviors

**Answer: D**

## Question: 663

Which combination of access controls provides the BEST physical protection for a server room?

A. User ID and PIN
B. PIN and smart card
C. Card with a magnetic stop and a shared PIN
D. Card with a magnetic strip and a smart card

**Answer: D**

## Question: 664

In an IS auditor's review of an organization s configuration management practices for software, which of the following is MOST important?

A. Post-implementation review reports from development efforts
B. Service level agreements (SLAs) between the IT function and users
C. Organizational policies related to release management
D. Software rental contracts or lease agreements

**Answer: C**

## Question: 665

To preserve chain-of-custody following an internal server compromise, which of the following should be the FIRST step?

A. Trace the attacking route.
B. Replicate the attack using the remaining evidence.
C. Take a system image including memory dump.
D. Safely shut down the server.

**Answer: C**

## Question: 666

A multinational organization is integrating its existing payroll system with a human resource information system. Which of the following should be of GREATEST concern to the IS auditor?

A. Application interfaces
B. Scope creep
C. System documentation
D. Currency conversion

**Answer: A**

## Question: 667

An organization with high security requirements is evaluating the effectiveness of biometric systems. Which of the following performance indicators is MOST important?

A. False-identification rate (FIR)
B. Equal-error rate (EER)
C. False-rejection rate (FRR)
D. False-acceptance rate (FAR)

**Answer: D**

## Question: 668

Which of the following is the GREATEST risk posed by denial-of-service attacks?

A. Confidential information leakage
B. Unauthorized access to the systems
C. Loss of integrity and corruption of databases
D. Loss of reputation and business

**Answer: D**

## Question: 669

The risk that the IS auditor will not find an error that has occurred is identified by which of the following terms?

A. Prevention
B. Inherent
C. Detection
D. Control

**Answer: D**

## Question: 670

An IS auditor finds that corporate mobile devices used by employees have varying levels of password settings. Which of the following would be the BEST recommendation?

A. Update the acceptable use policy for mobile devices.
B. Encrypt data between corporate gateway and devices.
C. Notify employees to set passwords to a specified length
D. Apply security policy to the mobile devices.

**Answer: D**

## Question: 671

An organization's IT security policy states that user ID's must uniquely identify individual's and that user should not disclose their passwords. An IS auditor discovers that several generic user ID's are being used. Which of the following is the MOST appropriate course of action for the auditor?

A. Recommend a change in security policy.
B. Include the finding in the final audit report.
C. Investigate the noncompliance.
D. Recommend disciplinary action.

**Answer: C**

## Question: 672

The purpose of data migration testing is to validate data:

A. retention.
B. completeness.
C. availability.
D. confidentiality.

**Answer: B**

## Question: 673

The BEST access strategy while configuring a firewall would be to:

A. permit access to all and log the activity.
B. deny access to all except authorized programs.
C. deny access to all but permit selected.
D. permit access to all but deny selected.

**Answer: C**

## Question: 674

An IS auditor concludes that a local area network (LAN) access security satisfactory. In reviewing the work, the audit manager should

A. Verify user management’s agreement with the findings
B. Assess whether the auditor had the appropriate skills to perform the work
C. Verify that the elements of an agreed upon audit plan have been addressed
D. Re-perform some steps of the audit to verify the quality of the work

**Answer: C**

## Question: 675

During the course of an audit, an IS auditor's organizational independence is impaired. The IS auditor should FIRST

A. inform senior management in writing and proceed with the audit
B. inform audit management of the situation.
C. proceed with the audit as planned after documenting the incident.
D. obtain the auditee s approval before continuing the audit.

**Answer: B**

## Question: 676

The results of a feasibility study for acquiring a new system should provide management with a clear understanding of:

A. how hardware selection criteria are aligned with the IS strategic plan.
B. critical application systems' utilization of computer resources.
C. the approach to meeting data processing needs.
D. application security over critical data processing.

**Answer: A**

## Question: 677

An organization has recently acquired and implemented intelligent-agent software for granting loans to customers. During the post implementation review, which of the following would be the KEY procedure for the IS auditor to perform?

A. Review system documentation to ensure completeness.
B. Ensure that a detection system designed to verify transaction accuracy is included.
C. Review input and output control reports to verify the accuracy of the system decisions.
D. Review signed approvals to ensure responsibilities for decisions of the system are welldefined.

**Answer: C**

## Question: 678

An IS auditor is reviewing IT policies and found that most policies have not been reviewed in over 3 years. The MOST significant risk is that the policies do not reflect.

A. The vision of the CEO
B. Current industry best practices
C. The mission of the organization
D. Current legal requirements

**Answer: D**

## Question: 679

What is the PRIMARY objective of implementing data classification?

A. Establish appropriate encryption methods.
B. Establish appropriate data protection methods.
C. Employ data leakage prevention tools.
D. Create awareness among users.

**Answer: B**

## Question: 680

Which of the following tools is MOST helpful in estimating budgets for tasks within a large IT business application project?

A. Ganttchart
B. Balanced scorecard

C. Critical path methodology (CPM)
D. Function point analysis (FPA)

**Answer: D**

## Question: 681

Adopting a service-oriented architecture would MOST likely:

A. facilitate connectivity between partners,.
B. streamline all internal processes.
C. compromise application software security
D. inhibit integration with legacy systems.

**Answer: A**

## Question: 682

A transaction processing system interfaces with the general ledger. Data analytics has identified that some transactions are being recorded twice
in the general ledger. While management states a system fix has been implemented, what should the IS auditor recommend to validate the
interface is working in the future?

A. Perform periodic reconciliations.
B. Ensure system owner sign-off for the system fix.
C. Conduct functional testing.
D. Improve user acceptance testing (UAT).

**Answer: D**

## Question: 683

Which of the following is the MOST important step in the development of an effective IT governance action plan?

A. Setting up an IT governance framework for the process
B. Conducting a business impact analysis (BIA)
C. Measuring IT governance key performance indicators (KPIs)
D. Preparing a statement of sensitivity

**Answer: A**

## Question: 684

An organization uses a web server hosting critical applications. Which of the following would represent the HIGHEST risk regarding the
availability and integrity of the web server?

A. Not applying program fixes on a regular basis
B. Placing the web server in the DMZ
C. Not disabling the server s external drives
D. Inadequate rotation of backups

**Answer: B**

## Question: 685

What is the BEST way for an IS auditor to address the risk associated with over-retention of personal data after identifying a large number of customer records retained beyond the retention period defined by law?

A. Recommend automatic deletion of records beyond the retention period
B. Schedule regular internal audits to identify records for deletion
C. Report the retention period noncompliance to the regulatory authority
D. Escalate the over-retention issue to the data privacy officer for follow up

**Answer: A**

## Question: 686

During audit planning, an IS auditor walked through the design of controls related to a new data loss prevention tool. It was noted that the tool will be configured to alert. IT management when large files are sent outside of the organization via email. What type of control will be tested?

A. Detective
B. Corrective
C. Directive
D. Preventive

**Answer: A**

## Question: 687

Which of the following will provide the GREATEST assurance to IT management that a quality management system (QMS) is effective?

A. A high percentage of stakeholders satisfied with the quality of IT
B. A high percentageofincidents being quickly resolved
C. A high percentage of IT employees attending quality training
D. A high percentageof IT processes reviewed by quality assurance

**Answer: B**

## Question: 688

A maturity model can be used to aid the implementation of IT governance by identifying:

A. improvement opportunities.
B. accountabilities.
C. performance drivers.
D. critical success factors.

**Answer: A**

## Question: 689

Which of the following methods should be used to effectively erase sensitive data from portable storage devices that are to be reused?

A. Using media sanitization software
B. Exposing the portable device to a magnetic field
C. Formatting the portable device
D. Overwriting the sensitive data

**Answer: B**

## Question: 690

Which of the following should be of MOST concern to an IS auditor evaluating a forensics program?

A. Forensic images are stored on removable media with encryption.

B. Forensic images are only stored for involuntarily terminated employees.
C. Forensic images are only maintained for 12 months.
D. Forensic images are stored on shared disks.

**Answer: D**

## Question: 691

An IS auditor is assessing an organization's implementation of a virtual network. Which of the following observations should be considered the
MOST significant risk?

A. Communication performance over the virtual network is not monitored.
B. Traffic over the virtual network is not visible to security protection devices.
C. Physical and virtual network configurations are not managed by the same team.
D. Virtual network devices are replicated and stored in offline mode.

**Answer: B**

## Question: 692

Which of the following would be the GREATEST concern when an organization's disaster recovery strategy utilizes a cold site?

A. The lack of hardware components availability
B. The lack of electrical power connections
C. The lack of appropriate environmental controls
D. The lack of networking infrastructure

**Answer: B**

## Question: 693

A CIO has asked an IS to implement several security controls for an organization's IT process and system. The auditor should:

A. Obtain approval from execute management for the implementation.
B. Communicate the conflict of interest to audit management.
C. Refuse due to independence issue
D. Perform the assignment and future audits with the due professional care.

**Answer: B**

## Question: 694

During the evaluation of a firm's newly established whistleblower system, an auditor notes several findings. Which of the following should be the
auditor's GREATEST concern?

A. The whistleblower system is only available during business hours.
B. New employees have not been informed of the whistleblower policy.
C. The whistleblower system does not track the time and date of submission.
D. The whistleblower's privacy is not protected.

**Answer: D**

## Question: 695

An IS auditor is mapping controls to risk for an accounts payable system What is the BEST control to detect errors in the system?

A. Quality control review of new payments
B. Management approval of payments
C. Input validation
D. Alignment of the process to business objectives

**Answer: C**

## Question: 696

An IS auditor is planning a risk-based audit of the human resources department. The department uses separate systems for its payroll, training
and employee performance review functions. What should the IS auditor do FIRST before identifying the key controls to be tested?

A. Determine the inherent risk related to each system.
B. Determine the number of samples to be tested for each system.
C. Assess the control risk associated with each system.
D. Identify the technical skills and resources needed to audit each system.

**Answer: A**

## Question: 697

An IS auditor previously worked in an organization s IT department and was involved with the design of the business continuity plan (BCP). The IS
auditor has now been asked to review this same BCP. The auditor should FIRST.

A. document the conflict in the audit report.
B. decline the audit assignment.
C. communicate the conflict of interest to the audit manager prior to starting the assignment.
D. communicate the conflict ofinterest to the audit committee prior to starting the assignment

**Answer: D**

## Question: 698

Which of the following reports can MOST effectively be used to analyze a systems performance problem?

A. Database usage log
B. Synchronization report
C. Console log
D. Utilization report

**Answer: C**

## Question: 699

During an audit, it is discovered that several suppliers with standing orders have been deleted from the supplier master file. Which of the
following controls would have BEST prevented such an occurrence?

A. Logical relationship check
B. Table look-ups
C. Existence check
D. Referential integrity

**Answer: D**

## Question: 700

To restore service at a large processing facility after a disaster, which of the following tasks should be performed FIRST?

A. Contact equipment vendors.
B. Activate the reciprocal agreement.
C. Launch the emergency action team.
D. Inform insurance company agents.

**Answer: C**

## Question: 701

Which of the following is the PRIMARY function of technology-driven enterprise architecture?

A. To determine how new technologies fit into existing networks and data flows
B. To re-engineer business processes to make better use of technology
C. To help develop project documentation and related business process roadmaps
D. To provide guidance on technological decisions in the context of business strategy

**Answer: D**

## Question: 702

A PRIMARY benefit derived by an organization employing control self-assessment (CSA) techniques s that CSA.

A. Allow management to relinquish responsibilities of control
B. Allows IS auditors 10 independently assess risk
C. Can identify high-risk areas for detailed review
D. Can be used as a replacement for traditional audits

**Answer: C**

## Question: 703

An organization is moving its on-site application servers to a service provider that operates a virtualized environment shared by multiple customers. Which of the following is the MOST significant risk to the organization?

A. Service provider access to organizational data
B. Competing workloads from other clients
C. Account hacking from other clients

D. Service provider limiting the right to audit

**Answer: B**

## Question: 704

Which of the following controls is MOST effective in detecting spam?

A. Denying transmission control protocol (TCP) connections in the mail server
B. Using heuristic filters based on the content of the message
C Refusing Internet protocol (IP) connections at the router
D. Registering the recipient with keepers of spam lists

**Answer: B**

## Question: 705

During a post-implementation review, a step in determining whether a project met user requirements is to review the:

A. completeness of user documentation.
B. integrity of key calculations.
C. effectiveness of user training.
D. change requests initiated after go-live.

**Answer: D**

## Question: 706

Which of the following is the MOST important control to help minimize the risk of data leakage from calls made to a business-to-business application programming interface (API)?

A. Deploying content inspection at the API gateway
B. Implementing API server clusters
C. Providing API security awareness training to developers
D. Implementing an API versioning system

**Answer: A**

## Question: 707

An organization has suffered a number of incidents in which USB flash drives with sensitive data have been lost. Which of the following would be
MOST effective in preventing loss of sensitive data?

A. Issuing encrypted USB flash drives to staff
B. Implementing a check-m/check-out process for USB flash drives
C. Increasing the frequency of security awareness training
D. Modifying the disciplinary policy to be more stringent

**Answer: A**

## Question: 708

Which of the following helps to ensure the integrity of data for an interface between a new billing system and an accounts receivable system?

A. Data files are encrypted during transmission.
B. Access to the data requires authentication.
C. Audit logs are available for 30 days.
D. Control totals are calculated.

**Answer: A**

## Question: 709

An IS auditor found that a company executive is encouraging employee use of social networking sites for business purposes. Which of the following recommendations would BEST help to reduce the risk of data leakage?

A. Providing education and guidelines to employees on use of social networking sites
B. Requiring policy acknowledgment and nondisclosure agreements signed by employees
C. Establishing strong access controls on confidential data
D. Monitoring employees social networking usage

**Answer: C**

## Question: 710

An advantage of object-oriented system development is that it:

A. decreases the need for system documentation.

B. partitions systems into a client/server architecture.
C. is suited to data with complex relationships.
D. is easier to code than procedural languages.

**Answer: D**

## Question: 711

Which of the following is the MOST effective way to minimize the risk of a SQL injection attack?

A. Reconfiguring content filtering settings
B. Performing activity monitoring
C. Using secure coding practices
D. Implementing an intrusion detection tool

**Answer: C**

## Question: 712

While auditing an IT department s cloud service provider, the IS auditor found that privileged access monitoring is not being performed as required by the contract. The provider disagrees with this issue and notes that compensating controls are in place. The IS auditor's NEXT course of action should be to:

A. review privileged access logs.
B. define a remediation plan.
C. recommend revising the service level agreement (SLA).
D. test compensating controls as part of the audit

**Answer: D**

## Question: 713

Which of the following documents would be MOST useful in detecting a weakness in segregation of duties?

A. Data flowdiagram
B. Entity-relationship diagram
C. Process flowchart
D. Systems flowchart

**Answer: B**

## Question: 714

Internal audit reports should be PRIMARILY written for and communicated to:

A. audit management as they are responsible for the quality of the audit.
B. external auditors, as they provide an opinion on the financial statements.
C. auditees, as they will eventually have to implement the recommendations
D. senior management as they should be informed about the identified risks.

**Answer: D**

## Question: 715

Which of the following has the GREATEST influence on the success of IT governance?

A. Alignment of IT strategies with the entity's vision
B. Clear, concise, and enforced IS policies
C. The CIO is a member of the audit committee
D. IT strategy is embedded in all risk management processes

**Answer: A**

## Question: 716

An IS auditor notes that a number of application plug-ins currently in use are no longer supported. Which of the following is the auditor's BEST
recommendation to management?

A. Implement role-based access controls.
B. Review content backup and archiving procedures.
C. Review on-boarding and off-boarding processes.
D. Conduct a vulnerability assessment to determine exposure.

**Answer: D**

## Question: 717

An organization has implemented an automated match between purchase orders, goods receipts, and invoices. Which of the following risks will this control BEST mitigate?

A. Customer discounts not being applied
B. Invalid payments being processed by the system
C. Delay of purchase orders
D. A legitimate transaction being paid multiple times

**Answer: B**

## Question: 718

An IS auditor discovers instances where software with the same license key is depbyed to multiple workstations, in breach of the licensing agreement. Which of the following is the auditor's BEST recommendation?

A. Evaluate the business case for funding of additional licenses.
B. Require business owner approval before granting software access
C. Remove embedded keys from offending packages.
D. Implement software licensing monitoring to manage duplications.

**Answer: D**

## Question: 719

Which of the following controls would BEST decrease the exposure if a password is compromised?

A. Password changes are forced periodically.
B. Passwords are encrypted.
C. Passwords are masked.
D. Passwords have format restrictions.

**Answer: B**

## Question: 720

An IS audit had identified that default passwords for a newly implemented application were not changed. During the follow-up audit which of the
following would provide the BEST evidence that the finding was effectively addressed?

A. Written confirmation from management that the passwords were changed
B. Screenshots of system parameters requiring password changes on next login
C. System-generated emails requiring application users to change passwords
D. Application log files that record the password changes

**Answer: D**

## Question: 721

To ensure efficient and economic use of limited resources in supporting a local area network (LAN) infrastructure, it is advisable to:

A. periodically rotate vendors to obtain the best price-to-performance ratio
B. standardize on a limited number of device models and software applications.
C. quickly upgrade to the latest hardware and software versions to take advantage of new features
D. recommend a variety of products so that user effectiveness and flexibility can be maximized.

**Answer: B**

## Question: 722

A vulnerability in which of the following virtual systems would be of GREATEST concern to the IS auditor?

A. The virtual application server
B. The virtual machine management server
C. The virtual antivirus server
D. The virtual file server

**Answer: B**

## Question: 723

A new regulation requires organizations to report significant security incidents to the regulator within 24 hours of identification. Which of the
following is the IS auditor s BEST recommendation to facilitate compliance with the regulation?

A. Enhance the alert functionality of the intrusion detection system (IDS).
B. Establish key performance indicators (KPIs) for timely identification of security incidents.
C. Include the requirement in the incident management response plan.
D. Engage an external security incident response expert for incident handling.

**Answer: C**

## Question: 724

Inherent risk rating are determined by assessing the impact and likelihood of a threat or vulnerability occurring:

A. Before the risk appetite Is established
B. After compensating have been applied
C. After internal controls are taken into account.
D. Before internal controls are taken into account.

**Answer: D**

## Question: 725

Which of the following will BEST protect the confidentiality of data stored on the hard drive of a laptop computer?

A. Biometric access control
B. A boot password
C. Physical locks and alarms
D. Encryption of the data

**Answer: D**

## Question: 726

Which of the following is the GREATEST risk resulting from conducting periodic reviews of IT over several years based on the same audit program?

A. The amount of errors with increase because the routine work promotes r\attentiveness.
B. Staff turnover in the audit department will increase because fieldwork becomes less interesting.
C. Detection risk is increased because auditees already know the audit program.
D. Audit risk is increased because the programs might not be adapted to the organization s current situation.

**Answer: D**

## Question: 727

Which of the following areas are the MOST likely cause of an application producing several erroneous reports?

A. A deficiency in user acceptance testing
B. A deficiency in IT resource allocation
C. A deficiency in patch management
D. A deficiency in database administration

**Answer: A**

## Question: 728

A database audit reveals an issue with the way data ownership for client data is defined. Which of the following roles should be accountable for this finding?

A. Business management
B. Database administrator
C. Information security management
D. Privacy manager

**Answer: A**

## Question: 729

An organization is developing a web portal using some external components. Which of the following should be of MOST concern to an IS auditor?

A. Some of the developers are located in another country.
The organization has not reviewed the components for known exploits.
C. Open-source components were integrated during development.
D. Staff require additional training in order to perform cede review.

**Answer: B**

## Question: 730

Which of the following IS functions can be performed by the same group or individual while still providing the proper segregation of duties?

A. Application programming and systems analysis
B. Computer operations and application programming
C. Security administration and application programming

D. Database administration and computer operations

**Answer: B**

## Question: 731

The IS security group is planning to implement single sign-on. What is the IS auditor's PRIMARY concern?

A. Integrated access rules will increase users' access privileges.
B. Integrated access rules will restrict users' access privileges.
C. Managing user IDs/passwords will require increased efforts.
D. Compromise of a user ID/password will yield more privileges

**Answer: D**

## Question: 732

Which of the following roles is ULTIMATELY accountable for the protection of an organization s information?

A. The board of directors
B. The chief information security officer (CISO)
C. The data owner
D. The chief information officer (CIO)

**Answer: A**

## Question: 733

Which of the following would be considered a corrective control when designing the security of a data center?

A. Security guards
B. Perimeter fence
C. Closed-circuit television (CCTV)
D. Fire extinguisher

**Answer: D**

## Question: 734

A potential risk of executing a program on an Internet site is that it may:

A. install executable code on the computer.
B. lack version control, which may result in the use of an older program.
C. overwrite system files with older versions
D. be browser-dependent, and therefore abort.

**Answer: B**

## Question: 735

Which of the following is the BCST way to determine the effectiveness of a recently installed intrusion detection system (IDS)?

A. Implement access control.
B. Conduct attack simulation.
C. Review audit logs.
D. inspect IDS configuration

**Answer: B**

## Question: 736

A legacy application is running on an operating system that is no longer supported by vendor, if the organization continues to use the current application, which of the application should be the IS auditor's GREATEST concern?

A. Inability to use the operating system due to potential licence issues
B. Increased cost of maintaining the system
C. Inability to update the legacy application database
D. Potential exploitation of zero-day vulnerabilities in the system

**Answer: D**

## Question: 737

An IS auditor is planning on utilizing attribute sampling to determine the error rate for health care claims processed. Which of the following factors will cause the sample size to decrease?

A. Tolerable error rate increase
B. Acceptable risk level decrease

C. Expected error rate increase
D. Population size increase

**Answer: A**

## Question: 738

A risk analysis is MOST useful when applied during which phase of the system development process?

A. Pre-implementation
B. Feasibility
C. Design
D. Testing

**Answer: B**

## Question: 739

Which of the following is the BEST way to transmit documents classified as confidential over the Internet?

A. Hashing the document contents and destroying the hash value
B. Sending documents as multiple packets over different network routes
C. Converting documents to proprietary format before transmission
D. Using a virtual private network (VPN)

**Answer: D**

## Question: 740

An organization is designing an application programming interface (API) for business-to-business data sharing
with a vendor. Which of the following is the BEST way to reduce the potential risk of data leakage?

A. Implement a policy to require data transfer over hypertext transfer protocol (HTTP)
B. Implement the API on a secure server and encrypt traffic between both organizations
C. Restrict the allowable number of API calls within a specified period
D. Conduct an independent review of the application architecture and service level agreements (SLAs)

**Answer: B**

## Question: 741

When reviewing a database supported by a third-party service provider, an IS auditor found minor control
deficiencies. The auditor should FIRST discuss recommendations with the:

A. service provider support team manager
B. organization's service level manager
C. organization's chief information officer (CIO)
D. service provider contract liaison

**Answer: B**

## Question: 742

A legacy application is running on an operating system that is no longer supported by the vendor. If the organization continues to use the current application, which of the following should be the IS auditor's GREATEST concern?

A. Potential exploitation of zero-day vulnerabilities in the system
B. Inability to update the legacy application database
C. Increased cost of maintaining the system
D. Inability to use the operating system due to potential license issues

**Answer: D**

## Question: 743

An organization has performance metrics to track how well IT resources are being used, but there has been little progress on meeting the organization's goals. Which of the following would be MOST helpful to determine the underlying reason?

A. Conducting a root cause analysis
B. Re-evaluating organizational goals
C. Re-evaluating key performance indicators (KPIs)
D. Conducting a business impact analysis (BIA)

**Answer: C**

## Question: 744

When determining the specifications for a server supporting an online application using more than a hundred endpoints, which of the following is the MOST important factor to be Considered?

A. Cost-benefit comparison between the available systems
B. High availability of different systems
C. Transaction volume estimate during peak periods
D. Reputation of the vendors and their customer base

**Answer: C**

## Question: 745

Which of the following is the BEST way to help ensure new IT implementations align with enterprise architecture principles and requirements?

A. Consider stakeholder concerns when defining the enterprise architecture.
B. Conduct enterprise architecture reviews as part of the change advisory board.
C. Perform mandatory post-implementation reviews of IT implementations.
D. Document the security view as part of the enterprise architecture.

**Answer: C**

## Question: 746

Which of the following is the PRIMARY objective of using a capability maturity model as a tool to communicate
audit results to senior management?

A. To evaluate management's action plan
B. To confirm audit findings
C. To illustrate improvement opportunities
D. To prioritize remediation efforts

**Answer: C**

## Question: 747

An audit of the quality management system (QMS) begins with an evaluation of the:

A. organization’s QMS policy
B. sequence and interaction of QMS processes
C. QMS processes and their application
D. QMS document control procedures

**Answer: A**

## Question: 748

Which of the following is an advantage of decentralized security administration?

A. Greater integrity
B. Faster turnaround
C. More uniformity
D. Better-trained administrators

**Answer: B**

## Question: 749

Which of the following observations should be of GREATEST concern to an IS auditor performing a review of
an organization’s IT governance structure?

A. The chief risk officer is also the chief information officer.
B. The chief information officer is prohibited from making capital decisions regarding IT.
C. The IT steering committee has oversight of the IT budget.
D. There are no IT subject matter expects on the board of directors.
D18912E1457D5D1DDCBD40AB3BF70D5D

**Answer: A**

## Question: 750

An IT steering committee assists the board of directors to fulfill IT governance duties by:

A. developing IT policies and procedures for project tracking.
B. focusing on the supply of IT services and products.
C. overseeing major projects and IT resource allocation.
D. implementing the IT strategy.

**Answer: D**

## Question: 751

Two servers are deployed in a cluster to run a mission-critical application. To determine whether the system
has been designed for optimal efficiency, the IS auditor should verify that:

A. the security features in the operating system are all enabled
B. the number of disks in the cluster meets minimum requirements
C. the two servers are of exactly the same configuration
D. load balancing between the servers has been implemented

**Answer: D**

## Question: 752

Which of the following is a distinguishing feature at the highest level of a maturity model?
D18912E1457D5D1DDCBD40AB3BF70D5D

A. There are formal standards and procedures.
B. Projects are controlled with management supervision.
C. A continuous improvement process is applied.
D. Processes are monitored continuously.

**Answer: C**

## Question: 753

An organization outsourced its IS functions. To meet its responsibility for disaster recovery, the organization
should:

A. delegate evaluation of disaster recovery to internal audit.
B. delegate evaluation of disaster recovery to a third party.
C. discontinue the maintenance of the disaster recovery plan (DRP).
D. coordinate disaster recovery administration with the outsourcing vendor.

**Answer: B**

## Question: 754

Which of the following audit procedures would BEST assist an IS auditor in determining the effectiveness of a
business continuity plan (BCP)?

A. Performing an assessment of BCP test documentation
B. Participating in BCP meetings held with user department managers
C. Performing a maturity assessment of BCP methodology against industry standards
D. Observing tests of the BCP performed at the alternate processing site

**Answer: D**

## Question: 755

In the review of a feasibility study for an IS acquisition, the MOST important step is to:

A. determine whether the cost-benefits are achievable.
B. ensure that a contingency plan is in place should the project fail.
C. ensure that the right to audit the vendor has been considered.
D. determine whether security and control requirements have been specified.

**Answer: C**

## Question: 756

What is the PRIMARY advantage of prototyping as part of systems development?

A. Maximizes user satisfaction
B. Reduces the need for compliance testing
C. Eliminates the need for internal controls
D. Increases accuracy in reporting

**Answer: A**

## Question: 757

What is the BEST indicator of successful implementation of an organization s information security policy?

A. Reduced number of noncompliance penalties incurred
B. Reduced number of successful phishing incidents
C. Reduced number of help desk calls
D. Reduced number of false-positive security events

**Answer: B**

## Question: 758

Due to the increasing size of a database, user access times and daily backups continue to increase. Which of the following would be the BEST way to address this situation?

A. Data modeling
B. Data purging
C. Data visualization
D. Data mining

**Answer: B**

## Question: 759

Which of the following is MOST important with regard to an application development acceptance test?

A. The quality assurance (QA) team is in charge of the testing process.
B. User management approves the test design before the test is started.
C. The programming team is involved in the testing process.
D. All data files are tested for valid information before conversion.

**Answer: D**

## Question: 760

Which of the following IT processes is likely to have the GREATEST inherent regulatory risk?

A. IT project management
B. Data management
C. Capacity management
D. IT resource management

**Answer: B**

## Question: 761

Which of the following is the PRIMARY reason for an IS auditor to issue an interim audit report?

A. To avoid issuing a final audit report
B. To enable the auditor to complete the engagement in a timely manner
C. To provide feedback to the auditee for timely remediation
D. To provide follow-up opportunity during the audit

**Answer: C**

## Question: 762

An IS auditor determines that a business impact analysis (BIA) was not conducted during the development of a
business continuity plan (BCP). What is the MOST significant risk that could result from this situation?

A. Responsibilities are not property defined.
B. Recovery time objectives (RTOs) are not correctly determined.
C. Key performance indicators (KPIs) are not aligned.
D. Critical business applications are not covered.

**Answer: D**

## Question: 763

Which of the following activities should occur after a business impact analysis (BIA)?

A. Identify threats to the IT environment
B. Identify critical applications
C. Analyze recovery options
D. Review the computing and user environment

**Answer: C**

## Question: 764

An IS auditor is following upon a finding that determined elevated administrator accounts for servers were not

being properly checked out and then back in after each use. Which of the following is the MOST appropriate
sampling technique to determine the scope of the problem?

A. Stratified sampling
B. Random sampling
C. Attribute sampling
D. Statistical sampling

**Answer: D**

## Question: 765

Which of the following is the BEST indication that an organization has achieved legal and regulatory compliance?

A. The board of directors and senior management accept responsibility for compliance.
B. An independent consultant has been appointed to ensure legal and regulatory compliance.
C. Periodic external and internal audits have not identified instances of noncompliance.
D. The risk management process incorporates noncompliance as a risk.

**Answer: C**

## Question: 766

Which of the following is the BEST point in time to conduct a post-implementation review (PIR)?

A. After a full processing cycle
B. Immediately after deployment
C. To coincide with annual PIR cycle
D. Six weeks after deployment

**Answer: D**

## Question: 767

Which of the following should be reviewed FIRST when planning an IS audit?

A. IS audit standards
B. Annual business unit budget
C. Recent financial information

D. The business environment

**Answer: C**

## Question: 768

Which of the following is the GREATEST cause for concern when an organization is planning to migrate business-critical applications to the cloud using a Platform as a Service (PaaS) model?

A. The organization will not manage operating system patches.
B. The cloud provider does not offer regional redundancy.
C. Compliance requirements are not being validated.
D. Application data will not be encrypted at rest.

**Answer: D**

## Question: 769

An IT governance framework provides an organization with:

A. assurance that there are surplus IT investments
B. assurance that there will be IT cost reductions
C. a basis for directing and controlling IT.
D. organizational structures to enlarge the market share through IT

**Answer: C**

## Question: 770

To create a digital signature in a message using asymmetric encryption, it is necessary to:

A. First use a symmetric algorithm for the authentication sequence.
B. encrypt the authentication sequence using a public key.
C. transmit the actual digital signature in unencrypted clear text.
D. encrypt the authentication sequence using a private key.

**Answer: B**

## Question: 771

During a post-incident review of a security breach, what type of analysis should an IS auditor expect to be
performed by the organization's information security team?

A. Gap analysis
B. Business impact analysis (BIA)
C. Qualitative risk analysis
D. Root cause analysis

**Answer: D**

## Question: 772

During the planning stage of compliance audit, an IS auditor discovers that the bank's inventory of compliance requirements does not include recent regulatory changes related to managing data risk. What would the auditor do FIRST?

A. Exclude recent regulatory changes from the audit scope
B. Discuss potential regulatory issues with the legal department
C. Ask management why the regulatory changes have not been included
D. Report the missing regulatory updates to the chief information officer (CIO)

**Answer: C**

## Question: 773

Which of the following is MOST important for successful incident response?

A. The timeless of attack recognition
B. The ability to trace the source of the attack
C. The quantity of data logged by the attack control tools
D. Blocking the attack route immediately

**Answer: A**

## Question: 774

Following an acquisition, it was decided that legacy applications subject to compliance requirements will continue to be used until they can be phased out. The IS auditor needs to determine where there are control
redundancies and where gaps may exist. Which of the following activities would be MOST helpful in making

this determination?

A. Control self-assessments
B. Risk assessment
C. Control testing
D. Control mapping

**Answer: D**

## Question: 775

Which of the following activities provides an IS auditor with the MOST insight regarding potential single person
dependencies that might exist withing the organization?

A. Reviewing user activity logs
B. Mapping IT processes to roles
C. Reviewing vacation patterns
D. Interviewing senior IT management

**Answer: B**

## Question: 776

An IS auditor is assigned to review the development of a specific application. Which of the following would be the MOST significant step following the feasibility study?

A. Attend project progress meetings to monitor timely implementation of the application.
B. Assist users in the design of proper acceptance-testing procedures.
C. Follow up with project sponsor for project's budgets and actual costs.
D. Review functional design to determine that appropriate controls are planned.

**Answer: D**

## Question: 777

Which of the following is MOST important for the successful establishment of a security vulnerability management program?

A. A comprehensive asset inventory
B. A tested incident response plan

C. An approved patching policy
D. A robust tabletop exercise plan

**Answer: C**

## Question: 778

An IS auditor is reviewing the results of a business process improvement project. Which of the following should
be performed FIRST?

A. Evaluate control gaps between the old and the new processes.
B. Develop compensating controls.
C. Document the impact of control weaknesses in the process.
D. Ensure that lessons learned during the change process are documented.

**Answer: A**

## Question: 779

Which of the following is the MOST reliable network connection medium in an environment where there is strong electromagnetic interface?

A. Fiber optic cable
B. Coaxial cable
C. Shielded twisted-pair cable
D. Wireless link

**Answer: A**

## Question: 780

The MAIN reason an organization's incident management procedures should include a post-incident review is to:

A. enable better reporting for executives and the audit committee
B. improve processes by learning from identified weaknesses
C. take appropriate action when procedures are not followed
D. ensure evidence is collected tor possible post-event litigation.

**Answer: B**

## Question: 781

Which of the following is MOST important for an IS auditor to consider when auditing a vulnerability scanning
software solution?

A. The scanning software was purchased from an approved vendor.
B. The scanning software was approved for release into production.
C. The scanning software covers critical systems.
D. The scanning software is cost-effective.

**Answer: C**

## Question: 782

The MOST important reason for documenting all aspects of a digital forensic investigation is that documentation:

A. provides traceability for independent investigation by third parties.
B. ensures compliance with corporate incident response policies.
C. ensures the process will be repeatable in future investigations.
D. meets IT audit documentation standards.

**Answer: A**

## Question: 783

While performing a risk-based audit, which of the following would BEST enable an IS auditor to identify and category risk?

A. Understanding the business environment
B. Understanding the control framework
C. Adopting qualitative risk analysis
D. Developing a comprehensive risk model

**Answer: A**

## Question: 784

A database administrator (DBA) extracts a user listing for an auditor as testing evidence. Which of the following will provide the GREATEST assurance that the user listing is reliable'

A. Obtaining sign-off from the DBA to attest that the list is complete
B. Requesting a copy of the query that generated the user listing
C. Requesting a query that returns the count of the users
D. Witnessing the DBA running the query in-person

**Answer: D**

## Question: 785

Which of the following is the GREATEST risk associated with in-house program development and customization?

A. The lack of secure coding expertise
B. The lack of a quality assurance function
C. The lack of a test environment
D. The lack of documentation for programs developed

**Answer: A**

## Question: 786

An IS auditor discovered abnormalities in a monthly report generated from a system upgraded six months ago. Which of the following should be the auditor's FIRST course of action?

A. Inspect source code for proof of abnormalities.
B. Schedule an access review of the system.
C. Perform a change management review of the system
D. Determine the impact of abnormalities in the report

**Answer: D**

## Question: 787

Which of the following is a prerequisite to help ensure that IS hardware and software support the delivery of mission-critical functions?

A. Control over IS infrastructure expenditure
B. A comprehensive IS applications architecture

C. Documented emergency change procedures
D. An independent audit of the process

**Answer: D**

## Question: 788

An IS auditor is assigned to review the IS department's quality procedures. Upon contacting the IS manager,
the auditor finds that there is an informal unwritten set of standards. Which of the following should be the
auditor's NEXT action?

A. Finalize the audit and report the finding.
B. Make recommendations to IS management as to appropriate quality standards.
C. Postpone the audit until IS management implements written standards.
D. Document and test compliance with the informal standards.

**Answer: A**

## Question: 789

Which of the following threats is MOST effectively controlled by a firewall?

A. Network congestion
B. Denial of service (DoS) attack
C. Network sniffing
D. Password cracking

**Answer: B**

## Question: 790

Which of the following would present the GREATEST risk to the effectiveness of a security operations center
for a global financial institution processing transactions 24×7?

A. Incident response reporting is based on open source software.
B. Incident response is conducted from a single location during normal business hours.
C. Correlation of events excludes logs for pre-production systems.
D. The incident response function is outsourced to a third-party provider.

**Answer: B**

## Question: 791

Which of the following is MOST likely to be included in a post-implementation review?

A. Test results
B. Results of live processing
C. Development methodology
D. Current sets of test data

**Answer: B**

## Question: 792

Which of the following controls BEST ensures appropriate segregation of duties within an accounts payable
department?

A. Ensuring that audit trails exist for transactions
B. Restricting access to update programs to accounts payable staff only
C. Restricting program functionality according to user security profiles
D. Including the creator's user ID as a field in every transaction record created

**Answer: A**

## Question: 793

Which of the following is an effective way to ensure the integrity of file transfers in a peer-to-peer (P2P) computing environment?

A. Connect the client computers in the environment to a jump server.
B. Ensure the files transferred through an intrusion detection system (IDS).
C. Encrypt the packets shared between peers within the environment.
D. Associate a message authentication code with each file transferred.

**Answer: C**

## Question: 794

Which of the following should an IS auditor review FIRST when planning a customer data privacy audit?

A. Legal and compliance requirements
B. Customer agreements
C. Organizational policies and procedures
D. Data classification

**Answer: C**

## Question: 795

Which of the following would provide the MOST useful input to IS audit management when developing an
action plan for improving internal audit's performance?

A. Feedback from departments that have participated in IS audits
B. Industry benchmarking analysis
C. An external quality assessment review
D. Results train an improvement initiative overseen by executive management

**Answer: C**

## Question: 796

Due to limited storage capacity, an organization has decided to reduce the actual retention period for media
containing completed low-value transactions. Which of the following is MOST important for the organization to
ensure?

A. The policy includes a strong risk-based approach.
B. The retention period allows for review during the year-end audit.
C. The total transaction amount has no impact on financial reporting.
D. The retention period complies with data owner responsibilities.

**Answer: A**

## Question: 797

An organization’s audit charter should:

A. set the enterprise strategic direction.

B. detail the audit objectives.
C. define the auditors' right to access information.
D. include the IS audit plan.

**Answer: B**

## Question: 798

At which stage of the software development life cycle should an organization identity privacy considerations?

A. Design
B. Testing
C. Development
D. Requirements

**Answer: D**

## Question: 799

During a review of operations, it is noted that during a batch update, an error was detected and the database
initiated a roll-back. An IT operator stopped the roll-back and re-initiated the update. What should the operator
have done PRIOR to re-initiating the update?

A. Determined the cause of the error
B. Obtained approval before re-initiating the update
C. Allowed the roll-back to complete
D. Scheduled the roll-back for a later time

**Answer: C**

## Question: 800

IS audit is asked 10 explain how local area network (LAN) servers can contribute to a rapid dissemination of viruses. The IS auditor's BEST response is that:

A. the server's software is the prime target and is the first to be infected
B. the server's operating system exchanges data with each station starting at every logon.
C. the server's file sharing function facilitates the distribution of files and applications.
D. users of a given server have similar usage of applications and files.

**Answer: B**

## Question: 801

Which of the following would BEST detect that a distributed-denial-of-service attack (DDoS) is occurring?

A. Server crashes
B. Penetration testing
C. Automated monitoring of logs
D. Customer service complaints

**Answer: D**

## Question: 802

A change to the scope of an IT project has been formally submitted to the project manager. What should the
project manager do NEXT?

A. Update the project plan to reflect the change in scope
B. Discuss the change with the project team and determine if it should be approved
C. Escalate the change to the change advisory board for approval
D. Determine how the change will affect the schedule and budget

**Answer: D**

## Question: 803

An organization allows employee use of personal mobile devices for corporate email. Which of the following
should be the GREATEST IS audit concern?

A. Email forwarding to private devices requires excessive network bandwidth
B. There is no corporate policy for the acceptable use of private devices
C. There is no adequate tracking of the working time spent out-of-hours
D. The help desk is not able to fully support different kinds of private devices

**Answer: B**

## Question: 804

Which of the following IS audit findings should be of GREATEST concern when preparing to migrate to a new core system using a direct cut-over?

A. informal management approval to 90 live
B. Lack of a rollback strategy for the system go-live
C. Plans to use some workarounds for an extended period after go-live
D. incomplete test cases for some critical reports

**Answer: B**

## Question: 805

Which of the following BEST helps to ensure data integrity across system interfaces?

A. Environment segregation
B. System backups
C. Reconciliations
D. Access controls

**Answer: D**

## Question: 806

During an audit of a mission-critical system hosted in an outsourced data center, an IS auditor discovers that contracted routine maintenance for the alternate power generator was not performed. Which of the following should be the auditor's MAIN concern?

A. Fraudulent behavior by the outsourcer charging for work not performed
B. Failure of the alternate power generator during a power outage
C. High repair costs if faulty generator parts are not detected in a timely manner
D. Loss of warranty due to lack of system maintenance

**Answer: B**

## Question: 807

An IS auditor is auditing the infrastructure of an organization that hosts critical applications withing a virtual
environment. Which of the following is MOST important for the auditor to focus on?

A. The ability to copy and move virtual machines in real time
B. The controls in place to prevent compromise of the host
C. Issues arising from system management of a virtual infrastructure
D. Qualifications of employees managing the applications

**Answer: B**

## Question: 808

Which of the following is the BEST indication that an information security program is effective?

A. The number of reported and confirmed security incidents has increased after awareness training.
B. The security awareness program was developed following industry best practices.
C. The security team has performed a risk assessment to understand the organization’s risk appetite.
D. The security team is knowledgeable and uses the best available tools.

**Answer: A**

## Question: 809

After discussing findings with an auditee, an IS auditor is required to obtain approval of the report from the
CEO before issuing it to the audit committee. This requirement PRIMARILY affects the IS auditor's:

A. judgment
B. effectiveness
C. independence
D. integrity

**Answer: C**

## Question: 810

An IS auditor concludes that a local area network's (LAN's) access security is satisfactory. In reviewing the work, the audit manager should:

A. re-perform some steps of the audit to verify the quality of the work
B. verify user management's agreement with the findings

C. assess whether the auditor had the appropriate skills to perform the work
D. verify that the elements of an agreed-upon audit plan have been addressed.

**Answer: D**

## Question: 811

An IS auditor is asked to review a large organization's change management process. Which of the following practices presents the GREATEST risk?

A. Change management tickets do not contain specific documentation.
B. Emergency code changes are promoted without user acceptance testing.
C. Transaction data changes can be made by a senior developer.
D. A system administrator performs code migration on planned downtime.

**Answer: D**

## Question: 812

Which of the following should be an IS auditor's GREATEST consideration when scheduling follow-up activities for agreed-upon management responses to remediate audit observations?

A. Business interruption due to remediation
B. IT budgeting constraints
C. Risk rating of original findings
D. Availability of responsible IT personnel

**Answer: C**

## Question: 813

While reviewing similar issues in an organization s help desk system, an IS auditor finds that they were analyzed independently and resolved differently This situation MOST likely indicates a deficiency in:

A. problem management
B. IT service level management
C. change management
D. configuration management

**Answer: A**

## Question: 814

Reorganization of databases is undertaken PRIMARILY to:

A. reduce backout and recovery times.
B. improve data access and retrieval times.
C. reduce simultaneous update time and index validation
D. eliminate duplicates and perform data backup.

**Answer: B**

## Question: 815

During an audit of the organization's data privacy policy, the IS auditor identified that only some IT application databases have encryption in place. What should be the auditors
FIRST action?

A. Assess the resources required to implement encryption to unencrypted databases.
B. Review the most recent database penetration testing results.
C. Determine whether compensating controls are in place
D. Review a comprehensive list of databases with the information they contain.

**Answer: D**

## Question: 816

Which of the following is the BEST way to evaluate the effectiveness of access controls to an internal network?

A. Perform a system penetration rest
B. Test compliance with operating procedures
C. Review access rights.
D. Review router configuration tables

**Answer: A**

## Question: 817

Which of the following is the MOST important difference between end-user computing (EUC) applications and

traditional applications?

A. Traditional application documentation is typically less comprehensive than EUC application documentation.
B. Traditional applications require roll-back procedures whereas EUC applications do not.
C. Traditional applications require periodic patching whereas EUC applications do not.
D. Traditional application input controls are typically more robust than EUC application input controls.

**Answer: D**

## Question: 818

The BEST reason for implementing a virtual private network (VPN) is that it:

A. eases the implementation of data encryption.
B. allows for public use of private networks.
C. enables use of existing hardware platforms.
D. allows for private use of public networks.

**Answer: D**

## Question: 819

Which of the following mechanisms for process improvement involves examination of industry best practice?

A. Continuous improvement
B. Knowledge management
C. Business process reengineering (BPR)
D. Benchmarking
D18912E1457D5D1DDCBD40AB3BF70D5D

**Answer: D**

## Question: 820

Stress testing should ideally be carried out under a:

A. production environment with test data.
B. test environment with test data.
C. production environment with production workloads.
D. test environment with production workloads.

**Answer: A**

## Question: 821

Which of the following is the GREATEST advantage of using a framework to guide an organization's governance of IT?

A. It enables consistency when making strategic IT investments across the organization.
B. It enables better management of the annual IT budget provided by the board of directors.
C. It enables improvements to the security of high-risk systems in the organization.
D. It enables the achievement of service levels between IT and true business departments.

**Answer: A**

## Question: 822

A retirement system verifies that the field for employee status has either a value of A (for active) or R (for retired). This is an example of which type of check?

A. Limit
B. Completeness
C. Existence
D. Validity

**Answer: D**

## Question: 823

Which of the following would be of MOST concern when determining if information assets are adequately
safeguard during transport and disposal?

A. Lack of password protection
B. Lack of recent awareness training
C. Lack of appropriate data classification
D. Lack of appropriate labeling

**Answer: C**

## Question: 824

A configuration management audit identified that predefined automated procedures are used when deploying
and configuring application infrastructure in a cloud-based environment. Which of the following is MOST important for the IS auditor to review?

A. Contracts of vendors responsible for maintaining provisioning tools
B. Processes for making changes to cloud environment specifications
C. Storage location of configuration management documentation
D. Number of administrators with access to cloud management consoles

**Answer: D**

## Question: 825

A retailer normally uses a scanner to read product labels and input product codes and prices. The unit is not
functioning and staff are keying information manually. With respect to the accuracy of the input, it is likely that:

A. audit risk has increased.
B. control risk has increased.
C. inherent risk has decreased.
D. detection risk has decreased.

**Answer: B**

## Question: 826

Which of the following should an IS auditor expect to find in an organization s information security policies?

A. Secure coding procedures
B. Authentication requirements
C. Security configuration settings
D. Asset provisioning lifecycle

**Answer: B**

## Question: 827

In an online application, which of the following would provide the MOST information about the transaction audit
trail?

A. File layouts
B. System/process flowchart
C. Source code documentation
D. Data architecture

**Answer: C**

## Question: 828

When removing a financial application system from production, which of the following is MOST important?
D18912E1457D5D1DDCBD40AB3BF70D5D

A. Media used by the retired system has been sanitized.
B. Data retained for regulatory purposes can be retrieved.
C. End-user requests for changes are recorded and tracked.
D. Software license agreements are retained.

**Answer: A**

## Question: 829

Which of the following provides the BEST evidence that network filters are functioning?
D18912E1457D5D1DDCBD40AB3BF70D5D

A. Reviewing network configuration rules
B. Reviewing network filtering policy
C. Performing network port scans
D. Analyzing network performance

**Answer: C**

## Question: 830

Which of the following test approaches would utilize data analytics to test a dual approval payment control?

A. Review payments completed in the past month that do not have a unique approver.
B. Attempt to complete a payment without a secondary approval.
C. Review users within the payment application who are assigned an approver role.
D. Evaluate configuration settings for the secondary approval requirements.

**Answer: B**

## Question: 831

Which of the following is the BEST indication that an organization's vulnerability identification capability has
achieved a high level of maturity?

A. The organization collaborates with relevant partners to correlate vulnerability data.
B. Known application vulnerabilities are manually categorized and prioritized.
C. Vulnerability management tools are tailored for specific operating systems.
D. Tools are in place to periodically identity new and updated vulnerabilities.

**Answer: C**

## Question: 832

Which of the following cloud deployment models would BEST meet the needs of a startup software development organization with limited initial capital?

A. Community
B. Public
C. Hybrid
D. Private

**Answer: C**

## Question: 833

An audit report notes that terminated employees have been retaining their access rights after their departure.
Which of the following strategies would BEST ensure that obsolete access rights are identified in a timely manner?

A. Delete user IDs at a predetermined date after their creation.
B. Automatically delete user IDs after they are unused for a predetermined time.
C. Implement an automated interface with the organization's human resources system.
D. Require local supervisors to initiate connection.

**Answer: C**

## Question: 834

An organization has made a strategic decision to split into separate operating entities to improve profitability.
However, the IT infrastructure remains shared between the entities. Which of the following would BEST help to
ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan?

A. Increasing the frequency of risk-based IS audits for each business entity
B. Revising IS audit plans to focus on IT changes introduced after the split
C. Conducting an audit of newly introduced IT policies and procedures
D. Developing a risk-based plan considering each entity's business processes
D18912E1457D5D1DDCBD40AB3BF70D5D

**Answer: B**

## Question: 835

An IS auditor is reviewing the upgrading of an operating system. Which of the following would be the GREATEST audit concern?

A. The lack of change control
B. The lack of malware protection
C. The lack of release notes
D. The lack of activity logging

**Answer: A**

## Question: 836

An organization has begun using social media to communicate with current and potential clients. Which of the
following should be of PRIMARY concern to the auditor?

A. Using a third-party provider to host and manage content
B. Lack of guidance on appropriate social media usage and monitoring
C. Negative posts by customers affecting the organization's image
D. Reduced productivity of stuff using social media

**Answer: B**

## Question: 837

Which of the following would be the PRIMARY benefit of replacing physical keys with an electronic badge system for access to a data center?

A. Tracking employee work hours
B. Increasing reliability
C. Increasing accountability
D. Maintaining compliance

**Answer: C**

## Question: 838

The drives of a tile server are backed up at a hot site. Which of the following is the BEST way to duplicate the
files stored on the server for forensic analysis?

A. Capture a bit-by-bit image of the file server's drives.
B. Run forensic analysis software on the backup drive.
C. Create a logical copy of the file server's drives.
D. Replicate the server's volatile data to another drive.
D18912E1457D5D1DDCBD40AB3BF70D5D

**Answer: A**

## Question: 839

Which of the following would BEST deter the theft of corporate information from a laptop?

A. Install biometric access controls.
B. Encrypt all data on the hard drive.
C. Protect files with passwords.
D. Encrypt the file allocation table (FAT).

**Answer: B**

## Question: 840

Electrical surge protectors BEST protect from the impact of:

A. electromagnetic interference.
B. power outages.
C. sags and spikes
D. reduced voltage.

**Answer: C**

## Question: 841

Which of the following projects would be MOST important to review in an audit of an organizations financial statements?

A. Automation of operational risk management processes
B. Resource optimization of the enterprise resource planning (ERP) system
C. Security enhancements to the customer relationship database
D. Outsourcing of the payroll system to an external service provider

**Answer: D**

## Question: 842

Which of the following is the GREATEST risk of using a reciprocal site for disaster recovery?

A. Mismatched organizational security policies
B. Equipment compatibility issues at the site
C. Inability to test the recovery plans onsite
D. Inability to utilize the site when required

**Answer: C**

## Question: 843

Which of the following is the BEST way to mitigate the impact of ransomware attacks?

A. Backing up data frequently
B. Invoking the disaster recovery plan (DRP)
C. Requiring password changes for administrative accounts
D. Paying the ransom

**Answer: C**

## Question: 844

Which of the following presents the GREATEST concern when implementing data flow across borders?

A. Equipment incompatibilities
B. National privacy laws
C. Political unrest
D. Software piracy laws

**Answer: B**

## Question: 845

An IS auditor notes that several of a client's servers are vulnerable to attack due to open unused ports and
protocols. The auditor recommends management implement minimum security requirements. Which type of
control has been recommended?

A. Preventive
B. Corrective
C. Directive
D. Compensating

**Answer: A**

## Question: 846

An organization wants to classify database tables according to its data classification scheme. From an IS Auditor's perspective, the tables should be classified based on the:

A. number of end users with access to the table
B. frequency of updates to the table
C. descriptions of column names in the table
D. specific functional contents of each single table

**Answer: A**

## Question: 847

When implementing a software product (middleware) to pass data between local area network (LAN) servers
and the mainframe, the MOST critical control consideration is:

A. cross-platform authentication.
B. time synchronization of databases.
C. network traffic levels between platforms.
D. time-stamping of transactions to facilitate recovery.

**Answer: D**

## Question: 848

A security regulation requires the disabling of direct administrator access. Such access must occur through an intermediate server that holds administrator passwords for all systems d records all actions. An IS auditor s PRIMARY concern with this solution would be that:

A. it represents a single point of failure
B. segregation of duties is not observed.
C. it is not feasible to implement
D. access logs may not be maintained

**Answer: A**

## Question: 849

Following an IT audit, management has decided to accept the risk highlighted in the audit report. Which of the
following would provide the MOST assurance to the IS auditor that management is adequately balancing the
needs of the business with the need to manage risk?

A. Established criteria exist for accepting and approving risk.
B. Identified risk is reported into the organization's risk committee.
C. Potential impact and likelihood is adequately documented.
D. A communication plan exists for informing parties impacted by the risk.

**Answer: B**

## Question: 850

An IS auditor attempts to sample for variables in a population of items with wide differences in values but
determines that an unreasonably large number of sample items must be selected to produce the desired
confidence level. In this situation, which of the following is the BEST audit decision?
D18912E1457D5D1DDCBD40AB3BF70D5D

A. Allow more time and test the required sample
B. Select a judgmental sample
C. Select a stratified sample
D. Lower the desired confidence level

**Answer: D**

## Question: 851

Which of the following would provide the MOST important input during the planning phase for an audit on the
implementation of a bring your own device (BYOD) program?

A. Policies including BYOD acceptable use statements
B. Results of a risk assessment
C. An inventory of personal devices to be connected to the corporate network
D. Findings from prior audits

**Answer: A**

## Question: 852

What should an IS auditor review FIRST when assessing the results of a recent penetration test to identify potential vulnerabilities?

A. Number of critical issues found
B. Skill level of the network support staff
C. Incident response process
D. Parameters of the test

**Answer: D**

## Question: 853

An organization has outsourced the development of a core application. However, the organization plans to bring the support and future maintenance of the application back in-house. Which of the following findings should be the IS auditor's GREATEST concern?

A. A training plan for business users has not been developed.
B. The vendor development team is located overseas.
C. The cost of outsourcing is lower than in-house development
D. The data model is not dearly documented.

**Answer: D**

## Question: 854

Which of the following would be of GREATEST concern to an IS auditor when auditing a small organization's
purchasing department?

A. The organization lacks a purchasing officer with experience in purchasing activities.
B. Purchases can be approved after expenses have already been incurred.
C. Some members of the department can request and approve payments for purchase requests.
D. Purchasing procedures and processes have not been updated during the past two years.

**Answer: D**

## Question: 855

Which of the following is the KST source of information for assessing the effectiveness of IT process monitoring?

A. Real-time audit software
B. Performance data
C. Quality assurance (QA) reviews
D. Participative management techniques

**Answer: B**

## Question: 856

To mitigate the risk of exposing data through application programming interface (API) queries, which of the
following design considerations is MOST important?

A. Data minimalization
B. Data quality
C. Data retention
D. Data integrity

**Answer: D**

## Question: 857

Which of the following is an IS auditor's BEST recommendation for mitigating risk associated with rapid expansion of hosts within a virtual environment?

A. Limit access to the hypervisor operating system (OS) and administration console
B. Ensure quick access to updated images of a guest operating system for fast recovery
C. Consider using a third-party service provider to share the virtual machine (VM) risk
D. Implement policies and processes to control virtual machine (VM) lifecycle management

**Answer: A**

## Question: 858

Which of the following is the MOST effective way for an IS auditor to evaluate the creation and deletion of
administrative accounts in a virtual environment?

A. Review password management procedures.
B. Review accounts to determine access requirements.
C. Review resource management for capacity performance.
D. Review account provisioning and deprovisioning procedures.

**Answer: D**

## Question: 859

*Visit us athttps://www.examsboost.com/test/cisa/*

Which of the following is the BEST approach to verify that internal help desk procedures are executed in compliance with policies?

A. Test a sample of closed tickets.
B. Benchmark help desk procedures.
C. Evaluate help desk call metrics.
C. Interview end users

**Answer: A**

## Question: 860

What is an IS auditor's BEST course of action if informed by a business unit's representatives that they are too busy to cooperate with a scheduled audit?

A. Reschedule the audit for a time more convenient to the business unit.
B. Notify the chief audit executive who can negotiate with the head of the business unit.
C. Begin the audit regardless and insist on cooperation from the business unit.
D. Notify the audit committee immediately and request they direct the audit begin on schedule.

**Answer: B**

## Question: 861

Which of the following is the BEST way for an IS auditor to assess the effectiveness of backup procedures?

A. Review the backup schedule.
B. Evaluate the latest data restore.
C. Inspect backup logs.
D. Interview the data owner.

**Answer: B**

## Question: 862

Which of the following is the PRIMARY reason for an IS auditor to map out the narrative of a business process?

A. To verify the business process is as described in the engagement letter
B. To identify the resources required to perform the audit
C. To ensure alignment with organizational objectives

D. To gain insight into potential risks

**Answer: D**

## Question: 863

When preparing to evaluate the effectiveness of an organizations IT strategy, an IS auditor should FIRST review;

A. the IT governance framework.
B. the IT processes and procedures.
C. Information security procedures.
D. the most recent audit results.

**Answer: D**

## Question: 864

When migrating critical systems to a cloud provider, the GREATEST data security concern for an organization would be that data from different clients may be:

A. subject to different service level agreements (SLAs) for disaster recovery.
B. subject to varying government compliance regulations.
C. requested during a legal discovery process.
D. improperly separated from each other.

**Answer: D**

## Question: 865

While following up on a prior audit report, an IS auditor determines that a number of recommendations to
address critical findings have not been implemented as agreed. What is the BEST course of action for the auditor?

A. Reclassify the risk ratings of the original findings.
B. Propose revised implementation timelines.
C. Escalate to the appropriate level of management.
D. Revise the scope of the follow-up audit

**Answer: C**

## Question: 866

An IS auditor is performing a routine procedure to test for the possible existence of fraudulent transactions.
Given there is no reason to suspect the existence of fraudulent transactions, which of the following data analytics techniques should be employed?

A. Association analysis
B. Classification analysis
C. Anomaly detection analysis
D. Regression analysis

**Answer: C**

## Question: 867

An IS auditor finds that one employee has unauthorized access to confidential dat
a. The IS auditor's BEST
recommendation should be to:
A. reclassify the data to a lower level of confidentiality.
B. recommend corrective actions to be taken by the security administrator.
C. implement a strong password schema for users.
D. require the business owner to conduct regular access reviews.

**Answer: D**

## Question: 868

An organization has outsourced its data leakage monitoring to an Internet service provider (ISP). Which of the following is the BEST way for an IS auditor to determine the effectiveness of this service?

A. Review the data leakage clause in the SLA.
B. verify the ISP has staff to deal with data leakage.
C. Simulate a data leakage incident.
D. Review the ISP's external audit report

**Answer: C**

## Question: 869

Which of the following is the GREATEST benefit of implementing an incident management process?

A. Reduction in security threats
B. Opportunity for frequent reassessment of incidents
C. Reduction in the business impact of incidents
D. Reduction of cost by the efficient use of resources

**Answer: C**

## Question: 870

Which of the following ensures components of an IT system are identified and baselined, and that changes to them are implemented in a controlled manner?

A. Change management process
B. Configuration management process
C. Software versioning control
D. Restricted production access

**Answer: B**

## Question: 871

A small organization does not have enough employees to implement adequate segregation of duties in accounts payable. Which of the following is the BEST compensating control to mitigate the risk associated with this situation?

A. Supervisory review of logs to detect changes in vendors
B. Rotation of duties among existing personnel
C. Review of transactions exceeding a specific threshold
D. Regular reconciliation of key transactions approved by a supervisor

**Answer: A**

## Question: 872

During a business continuity audit, an IS auditor found that the business continuity plan (BCP) only covers critical processes. The auditor should:

A. recommend that the BCP consider all business processes.
B. assess the impact of processes not covered.
C. redefine the critical processes.
D. report findings to the chief executive officer (CEO).

**Answer: B**

*The business impact analysis needs to be either updated or revisited to assess the risk of not covering all processes in the plan. It is possible that the cost of including all processes might exceed the value of those processes; therefore, they should not be covered. An IS auditor should substantiate this by analyzing the risk.*

## Question: 873

Which of the following is MOST important for the successful completion of a new application system?

A. Appropriate training of system analysts
B. User participation in the project development
C. Steering committee approval of the new system
D. Completion of a positive cost-benefit analysis

**Answer: B**

## Question: 874

In reviewing the project timeline for a significant application software development project the IS auditor notes that no time was allocated for the design and performance of program code unit tests. Which of the following should the auditor recommend?

A. Unit test design should be performed after user testing is performed.
B. Unit test design should be performed before program coding begins.
C. Unit lest design should be performed before program specifications are defined.
D. Unit testing is not necessary since exhaustive user testing will be performed.

**Answer: B**

## Question: 875

Which of the following would provide the BEST evidence for use in a forensic investigation of an employee's hard drive?

A. Prior backups

B. Bit-stream copy of the hard drive
C. A file level copy of the hard drive
D. Memory dump to an external hard drive

**Answer: A**

## Question: 876

An organization has selected a web-based solution to reduce transaction costs and improve productivity. Before implementation, an IS auditor should ensure that the organization has:

A. addressed the level of risk exposure
B. validated the solution against the current IT infrastructure.
C. performed a vulnerability assessment.
D. Implemented electronic data interchange.

**Answer: A**

## Question: 877

Which of the following is the PRIMARY responsibility of an information owner?

A. Implementing access control policies
B. Assigning classification levels to information assets
C. Implementing periodic data backups
D. Designing the information classification scheme

**Answer: B**

## Question: 878

Within a payroll department, which of the following responsibilities should be assigned to two or more individuals to avoid a segregation of duties conflict?

A. Adding and removing new users of the payroll system
B. Viewing lists of terminated employees and editing payroll information
C. Approving payroll payments and inputting salary rates into the system
D. Reviewing time sheets and accessing bank statements for account reconciliation

**Answer: D**

## Question: 879

The risk that is created if a single sign-on is implemented for all systems is that a/an:

A. authorized user can bypass the security layers.
B. user tan bypass current access security.
C. user has equivalent access on all systems.
D. compromised password gives access to all systems.

**Answer: D**

## Question: 880

Which of the following should an IS auditor expect to find when reviewing IT security policy?

A. Virus protection Implementation strategies
B. An inventory of information assets
C. A risk-based classification of systems
D. Assigned responsibility for safeguarding company assets

**Answer: D**

## Question: 881

A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is MOST effective in detecting such an intrusion?

A. Using smart cards with one-time password
B. Configuring the router as a firewall
C. Installing Biometrics-based authentication
D. Periodically reviewing log files

**Answer: B**

## Question: 882

While evaluating an organization's program for tracking system interfaces and data transfers, the IS auditor notices the program does not record some of the ad hoc transfers that occur. Which of the following is the GREATEST potential risk?

A. Peer-to-peer data transfers may not be encrypted.
B. No repudiation controls may be Ineffective or nonexistent.
C. Some ad hoc transfers may not use secure FTP sites.
D. Management reports may be Incomplete.

**Answer: D**

## Question: 883

Which of the following is the MOST important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings?

A. Complexity of business processes identified in the audit
B. Peak activity periods for the business
C. Remediation dates included m management responses
D. Availability of IS audit resources

**Answer: C**

## Question: 884

The BEST way to evaluate the effectiveness of a newly developed application is to:

A. perform a post-implementation review,
B. review acceptance-testing results
C. analyze load-testing results,
D. perform a pre-implementation renew.

**Answer: B**

## Question: 885

When assessing a business case as part of a post-implementation review, the IS auditor MUST ensure that the:

A. feasibility of alternative project approaches has been assessed.
B. business case has not been amended since project approval.
C. amendments to the business case have been approved.

D. quality assurance measures have been applied throughout the project

**Answer: C**

## Question: 886

Which of the following is an advantage of using electronic data interchange (EDI)?

A. Data validation is provided by the service provider.
B. Contracts with the vendors are simplified.
C. Multiple inputs of the same document are allowed at different locations.
D. Transcription of information is reduced.

**Answer: D**

## Question: 887

When designing metrics for information security, the MOST important consideration is that the metrics:

A. track trends over time.
B. apply to all business units.
C. are easy to understand.
D. provide actionable data.

**Answer: A**

## Question: 888

Which of the following is the MOST critical step prior to performing a network penetration test?

A. Informing management of the potential risk involved with penetration testing
B. Identifying a scanning tool for use in identifying vulnerabilities
C. Communicating the location of the penetration test targets to management
D. Reviewing the result of previous penetration tests.

**Answer: A**

## Question: 889

Which of the following reflects inadequate segregation of duties?

A. The same employee who maintains, configures, and backs up servers also runs batch jobs.
B. The same employee who maintains and configures servers also monitors network event logs.
C. The same employee who builds and monitors databases also maintains and configures servers.
D. The same employee who maintains and configures servers also develops application software.

**Answer: C**

## Question: 890

Which of the following poses the GREATEST risk to data security and integrity in a cloud environment?

A. Data is transmitted using hypertext transfer protocol (HTTP).
B. Data backups are maintained with the cloud provider.
C. Data is not classified prior to transmission to the cloud provider.
D. Data regulations are not clearly defined for the cloud provider.

**Answer: C**

## Question: 891

When replacing a critical software application, which of the following provides for the LOWEST risk of interruption to business processes?

A. Big-bang implementation
B. Parallel implementation
C. Pilot implementation
D. Incremental implementation

**Answer: B**

## Question: 892

Which of the following should an IS auditor be MOST concerned with when a system uses ratio frequency identification (RFID)?

A. Scalability
B. Maintainability
C. Privacy
D. nonrepudiations

**Answer: A**

## Question: 893

Which of the following should be an IS auditor's PRIMARY consideration when reviewing a project to outsource data center hosting services?

A. Regulatory requirements regarding the location of data
B. Adherence to industry standards for ensuring integrity of data
C. The vendor's ability to meet established service level agreements (SLAs)
D. Existence of a right-to-audit clause in the vendor agreement

**Answer: A**

## Question: 894

Which of the following would have the GREATEST impact on defining the classification levels for electronic documents?

A. End user preferences
B. Document archival requirements
C. Volume of information
D. Value of information

**Answer: D**

## Question: 895

Which of the following control? MOST efficiently ensures that orders transmitted from a sales office to a production warehouse are received accurately and completely?

A. Data should be sent back to the originating site and compared to what was sent to production.
B. Continuity of numerical sequences for all sales orders should be checked.
C. Parity checking should be incorporated into all data transmissions.
D. Transaction totals and record counts should be sent and reconciled before transaction processing.

**Answer: D**

## Question: 896

An organization wants to reuse company-provided smartphones collected from staff leaving the organization. Which of the following would be the BEST recommendation?

A. The memory cards of the smartphones should be replaced.
B. Data should be securely deleted from the smartphones.
C. The SIM card and telephone number should be changed.
D. Smartphones should not be reused, but physically destroyed.

**Answer: B**

## Question: 897

When testing segregation of duties, which of the following audit techniques provides the MOST reliable evidence?

A. Interviewing managers and end users
B. Observing daily operations for the area in scope
C. Evaluating the department structure via the organizational chart
D. Reviewing departmental procedure handbooks

**Answer: B**

## Question: 898

During an audit of a payroll system, an IS auditor identifies that two employees share the same bank account. The auditor is concerned they may be ghost employees. Which of the following should the auditor do NEXT?

A. Advise payroll management to suspend both employees accounts until further investigated.
B. Draft a report with a finding that there may be ghost employees.
C. Notify the human resources executive immediately.
D. Conduct inquiries to determine whether the two employees have a relationship.

**Answer: D**

## Question: 899

Which of the following would provide the MOST assurance that an application will work in a live environment?

A. Walking through the programs to view the results of error processing
B. Processing of test data to prove that data can passed between individual programs

C. Walking through the programs to view the results of processing copies of production data
D. Processing of valid and erroneous data In an acceptance test environment

**Answer: D**

## Question: 900

An organization with high availability resource requirements is selecting a provider for cloud computing. Which of the following would cause the GREATEST concern to an IS auditor? The provider:

A. hosts systems for the organization's competitor.
B. does not store backup media offsite.
C. is not internationally certified for high availability.
D. deploys patches automatically without testing.

**Answer: D**

## Question: 901

Which of the following is the MOST important consideration when planning a penetration test for a financial management system?

A. The scanning will be cost efficient
B. The scope of the test was approved.
C. Vulnerability testing will also be performed.
D. The tester does not have any conflicts of interest

**Answer: D**

## Question: 902

Which of the following should an IS auditor recommend to facilitate the management of baseline requirements for hardening of firewalls?

A. Configuration management
B. Release management
C. Capacity management
D. Patch management

**Answer: A**

## Question: 903

When auditing the security architecture of an e-commerce environment, an IS auditor should FIRST review the:

A. criteria used for selecting the firewall.
B. location of the firewall within the network.
C. configuration of the firewall.
D. alternate firewall arrangements.

**Answer: A**

## Question: 904

An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party
service provider. Which of the following would be the BEST way to prevent accepting bad data?

A. Appoint data quality champions across the organization
B. Obtain error codes indicating failed data feeds
C. Purchase data cleansing tools from a reputable vendor
D. Implement business rules to reject invalid data

**Answer: B**

## Question: 905

Which of the following is the BEST type of backup to minimize the associated time and media?

A. Compressed full
B. Mirror
C. Incremental
D. Differential

**Answer: C**

## Question: 906

When determining the specifications for a server supporting an online application using more than a hundred endpoints, which of the following is the MOST important factor to be Considered?

A. Cost-benefit comparison between the available systems
B. High availability of different systems
C. Transaction volume estimate during peak periods
D. Reputation of the vendors and their customer base

**Answer: C**

## Question: 907

Which of the following presents the GREATEST security risk in a virtualized computing environment?

A. Some business users have not received appropriate training on the virtual desktop environment.
B. Physical access to the data center that hosts hardware for virtual machines is not logged.
C. Backups for sensitive data formats are not stored at an offsite location.
D. Passwords for the software that controls the operations of virtual machines are set to default.

**Answer: D**

## Question: 908

Which of the following is an example of a data analytics use case during the fieldwork phase of an IS audit?

A. Matching ingress records to egress records to identify tailgated access to sensitive IT areas
B. Evaluating security controls against globally recognized security frameworks
C. Applying data visualization techniques to generate s report to audit management
D. Assessing the audit universe to identify high-risk entities to be included in the annual audit plan

**Answer: A**

## Question: 909

Which of the following controls would BEST ensure that payroll system rate charges are valid?

A. Rate changes are reported to and independently verified by a manager
B. Rate change require visual verification before acceptance
C. Rate changes must be entered twice to ensure that they are entered correctly
D. Only a payroll department manager can input the new rate.

**Answer: A**

## Question: 910

An auditor is creating an audit program in which the objective is to establish the adequacy of personal data privacy controls in a payroll process. Which of the following would be MOST important to include?

A. Approval of data changes
B. User access provisioning
C. Segregation of duties controls
D. Audit logging of administrative user activity

**Answer: B**

## Question: 911

An IS auditor auditing the effectiveness of utilizing a hot site will MOST likely:

A. review reciprocal agreements
B. review logical access controls
C. evaluate physical access control
D. analyze system restoration procedures

**Answer: D**

## Question: 912

Which of the following would provide the BEST evidence of successfully completed batch uploads?

A. Reviewing process logs
B. Enforcing batch cut-off times
C. Using sequence controls
D. Sign-off on the batch journal

**Answer: A**

## Question: 913

A small organization is experiencing rapid growth and plans to create a new information security policy. Which of the following is MOST relevant to creating the policy?

A. Industry standards
B. The business objectives
C. The business impact analysis
D. Previous audit recommendations

**Answer: C**

## Question: 914

Which of the following is MOST important to helping incident response managers quickly and accurately estimate the overall business impact of security incidents?

A. Develop a communication plan and identity key business stakeholders to be notified.
B. Ensure the security Incident management team Is staffed with qualified Individuals.
C. Engage senior business management in determining seventy levels for escalation.
D. Map IT infrastructure to the business processes and client services they support.

**Answer: D**

## Question: 915

Which of the following requires a consensus by key stakeholders on IT strategic goals and objectives?

A. Benchmarking
B. Peer reviews
C. Balanced scorecards
D. Maturity models

**Answer: C**

## Question: 916

Which of the following should an IS auditor do FIRST when determining whether to employ data analytics in an audit?

A. Identify the business stakeholders.
B. Determine if the data is accessible.
C. Review the results of prior audits in the same area.
D. Review the data available in existing business reports

**Answer: D**

## Question: 917

The prioritization of incident response actions should be PRIMARILY based on which of the following?

A. Business impact
B. Scope of disaster
C. Availability of personnel
D. Escalation process

**Answer: A**

## Question: 918

Which of the following should be restricted from a network administrator's privileges in an adequately segregated H" environment?

A. Opening and closing network ports
B. Changing existing configurations for applications
C. Ensuring transmission protocols are functioning correctly
D. Monitoring network traffic and detecting anomalies

**Answer: A**

## Question: 919

Which of the following security mechanisms should be used to prevent disclosures of personally identifiable information (PH) when performing data analytics?

A. Tokenization
B. Segmentation
C. Encryption
D. Anonymization

**Answer: D**

## Question: 920

Which the following is MOST critical for the effective implementation of IT governance?

A. Documented policies
B. Strong risk management practices
C. Internal auditor commitment
D. Supportive corporate culture

**Answer: D**

## Question: 921

Which of the following is the BEST indicator of a mature quality management system (QMS)?

A. Projects are snowing continuous improvement
B. End users are satisfied with the outcome of IT projects.
C. Most IT projects have been completed on time and within budget.
D. Continuous improvement has been integrated into business processes.

**Answer: D**

## Question: 922

Which of the following should be performed immediately after a computer security incident has been detected and analyzed by an incident response team?

A. Categorize the incident
B. Eradicate the component that caused the incident
C. Assess the impact of the incident on critical systems.
D. Contain the incident before it spreads.

**Answer: D**

## Question: 923

Which of the following requirements in a document control standard would provide nonrepudiation to digitally signed legal documents?

A. All documents requiring digital signatures must be signed by both the customer and a witness.
B. Only secure file transfer protocol (SFTP) may be used for digitally signed documentation.
C. All digitally signed documents must be stored in an encrypted database.
D. All digital signatures must include a hashing algorithm.

**Answer: D**

## Question: 924

Which of the following factors will BEST promote effective information security management?

A. Senior management commitment
B. Identification and risk assessment of sensitive resources
C. Security awareness training
D. Security policy framework

**Answer: A**

## Question: 925

Which of the following is the BEST development methodology to help manage project requirements in a rapidly changing environment?

A. Prototyping
B. Iterative development process
C. Object-oriented system development
D. Waterfall development process

**Answer: B**

## Question: 926

An IT department installed critical patches provided by the vendor to HR production servers. Immediately after the installation was completed, the HR department called to report that none of its users could access the system, what should be the IT department's FIRST step in addressing this issue?

A. Follow back-out procedures
B. Troubleshoot the system and fix the issue.
C. Run system diagnostics on the staging servers.
D. Document the calls and user issues.

**Answer: A**

## Question: 927

Which of the following system deployments requires the cloud provider to assume the widest range of responsibilities for data protection?

A. Software as a Service (SaaS)
B. Platform as a Service (PaaS)
C. Database as a Service (DBaaS)
D. Infrastructure as a Service (IasS)

**Answer: A**

## Question: 928

A region where an organization conducts business has announced changes in privacy legislation. Which of the following should an IS auditor do FIRST to prepare for the changes?

A. Perform a gap analysis with current privacy procedures.
B. Provide suggested updates to the organization's privacy procedures.
C. Communicate the changes In privacy legislation to the legal department.
D. Design compensating controls to be in compliance with new privacy legislation.

**Answer: A**

## Question: 929

Which of the following key performance indicators (KPIs) provides the BEST indication of a security awareness campaign's effectiveness?

A. Percentage of attendees passing the awareness quiz
B. Reduced average rime for incident resolution
C. Decrease m the number of help desk calls
D. Increase in the number of reported security incidents

**Answer: D**

## Question: 930

The recovery time objective (RTO) is normally determined on the basis of the:

A. acceptable downtime of the alternate site,
B. risk of occurrence.
C. criticality of the systems affected.
D. cost of recovery of all systems.

**Answer: C**

## Question: 931

Which of the following is the MOST important factor when an organization is developing information security policies and procedures?

A. Compliance with relevant regulations
B. Cross-references between policies and procedures
C. Inclusion of mission and objectives
D. Consultation with management

**Answer: C**

## Question: 932

An IS auditor notes that application super-user activity was not recorded in system logs. What is the auditor's BEST course of action?

A. Investigate the reason for the lack of logging
B. Recommend a least privilege access model
C. Recommend activation of super user activity logging
D. Report the issue to the audit manager

**Answer: A**

## Question: 933

An IS auditor has been asked to advise on the design and implementation of IT management best practices Which of the following actions would impair the auditor's independence?

A. Implementing risk response on management's behalf
B. Evaluating the risk management process
C. Providing consulting advice for managing applications
D. Designing an embedded audit module

**Answer: A**

## Question: 934

Which of the following is MOST important to the effective management of an end user developed application?

A. Implementing best practice folder structures
B. Assigning risk ratings based on probability and impact
C. Stress testing the application through use of data outliers
D. Continuous monitoring to facilitate prompt escalation of issues

**Answer: B**

## Question: 935

An IT management group has developed a standardized security control checklist and distributed it to the control self-assessors in each organizational unit. Which of the following would be the GREATEST risk m this approach?

A. Business-specific vulnerabilities may be overlooked.
B. Delayed feedback may increase exposures
C. Assessors may manipulate the results
D. Over time the checklist may become outdated.

**Answer: A**

## Question: 936

When engaging services from external auditors, which of the following should be established FIRST?

A. Termination conditions agreements
B. Nondisclosure agreements
C. Service level agreements
D. Operational level agreements

**Answer: B**

## Question: 937

An IS auditor finds multiple situations where the help desk resolved security incidents without notifying IT security as required by policy. Which of the following is the BEST audit recommendation?

A. Reinforce the incident escalation process

B. Redesign the help desk reporting process.
C. Have IT security review problem management policy.
D. Display the incident response hotline in common areas.

**Answer: B**

## Question: 938

Which of the following is the MOST important requirement for an IS auditor to evaluate when reviewing a transmission of personally identifiable information between two organizations?

A. Timeliness
B. Completeness
C. Accuracy
D. Necessity

**Answer: D**

## Question: 939

A typical network architecture used for e-commerce, a load balancer is normally found between the:

A. routers and the web servers.
B. mail servers and the mail repositories
C. databases and the external gateways,
D. users and the external gateways.

**Answer: C**

## Question: 940

During a network security review the system log indicates an unusually high number of unsuccessful login attempts Which of the following sampling techniques is MOST appropriate for selecting a sample of user IDs for further investigation?

A. Variable
B. Monetary unit
C. Stratified
D. Attribute

**Answer: D**

## Question: 941

During a vulnerability assessment, an IS auditor finds a high-risk vulnerability in a public-facing web server used to process online customer orders via credit card. The IS auditor could FIRST:

A. notify management.
B. document the finding in the report
C. redesign the customer order process.
D. suspend credit card processing.

**Answer: A**

## Question: 942

An organization is considering replacing physical backup tapes stored offsite with real-time on-line backup to a storage area network (SAN) located in the primary data center. Which of the following is the GREATEST risk?

A. Backups may require excessive storage space.
B. Implementation could cause significant cost increases.
C. Archived data may not satisfy data retention requirements.
D. A single disaster could cause significant data loss

**Answer: D**

## Question: 943

Which of the following is the MOST critical characteristic of a biometric system?

A. Registration time
B. Throughput rate
C. Accuracy
D. Ease of use

**Answer: C**

## Question: 944

Which of the following group is MOST likely responsible for the implementation of IT projects?

A. IT steering committee
B. IT strategy committee
C. IT compliance committee
D. IT governance committee

**Answer: A**

## Question: 945

During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be MOST concerned with the:

A. differences in IS policies and procedures
B. maintenance of hardware and software compatibility
C. frequency of system testing
D. allocation of resources during an emergency

**Answer: A**

## Question: 946

An IS auditor has found that a vendor has gone out of business and the escrow has an older version of the source code What is the auditor's BEST recommendation for the organization?

A. Prepare a maintenance plan that will support the application using the existing code.
B. Bring the escrow version up to date
C. Continue using the existing application since it meets the current requirements.
D. Undertake an analysis to determine the business risk.

**Answer: B**

## Question: 947

A technology service organization has recently acquired a new subsidiary. What should be the IS auditor's NEXT course of action when considering the impact on the development of the IT audit plan?

A. Review the revised business impact analysis (B1A).
B. Proceed with the current audit plan.
C. Include the new systems in the audit plan.
D. Perform a risk assessment.

**Answer: D**

## Question: 948

The PRIMARY benefit of using secure shell (SSH) to access a server on a network is that it:

A. provides confidentiality of transmitted data
B. prevents man-in-the-middle attacks
C. provides better session reliability
D. facilitates communication across platforms.

**Answer: A**

## Question: 949

The PRIMARY reason an IS department should analyze past incidents and problems is to:

A. determine if all incidents and problems are reported
B. assess help desk performance
C. assign responsibility for problems.
D. identify the causes of recurring incidents and problems.

**Answer: D**

## Question: 950

Attribute sampling is BEST suited to estimate:

A. the total error amount in the population
B. compliance with approved procedures
C. whether a recorded balance is within limits of materiality,
D. the true monetary value of a population

**Answer: C**

## Question: 951

Digital signatures are an effective control method for information exchange over an insecure network because they:

A. enable non repudiation
B. authenticate the user biometrically
C. are under the sole custody of the receiver
D. are constant over time

**Answer: A**

## Question: 952

Which of the following would be MOST important to include in a data security policy to adequately manage the privacy of customer information?

A. Information classification criteria
B. Data ownership
C. Encryption technology
D. Backup strategy

**Answer: A**

## Question: 953

Which of the following scenarios would enable a forensic investigation?

A. Incident response team members extracted the logs showing the suspicious activity and added their notes before submitting for investigation.
B. The media in question was preserved using imaging, and chain of custody was documented according to the organization's incident response plan.
C. The suspected computer was rebooted, and the evidence log file was converted to a readable format for further analysis.
D. The incident response team prepared a final report for the forensic investigator and deleted the original file securely to avoid further damage.

**Answer: B**

## Question: 954

Which of the following would be the MOST appropriate reason for an organization to purchase fault-tolerant hardware?

A. Improving system performance
B. Reducing hardware maintenance costs
C. Minimizing business loss
D. Compensating for the lack of contingency planning

**Answer: C**

## Question: 955

As part of an IS audit, the auditor notes the practices listed below.
Which of the following would be a segregation of duties concern?

A. Operators are degaussing magnetic tapes during night shifts
B. System programmers have logged access to operating system parameters.
C. System programmers are performing the duties of operators.
D. Operators are acting as tape librarians on alternate shifts.

**Answer: C**

## Question: 956

During an audit of identity and access management, an IS auditor finds that the engagement audit plan does not include the testing of controls that regulate access by third parties. Which of the following would be the auditor's BEST course of action?

A. Add testing of third-party access controls to the scope of the audit.
B. Escalate the deficiency to audit management.
C. Plan to test these controls in another audit.
D. Determine whether the risk has been identified in the planning documents.

**Answer: D**

## Question: 957

Which of the following provides the BEST audit evidence that a firewall is configured in compliance with the organization's security policy?

A. Analyzing how the configuration changes are performed
B. Analyzing log files
C. Performing penetration testing
D. Reviewing the rule base

**Answer: A**

## Question: 958

Which of the following IS functions can be performed by the same group or individual while still providing the proper segregation of duties?

A. Application programming and systems analysis
B. Computer operations and application programming
C. Security administration and application programming
D. Database administration and computer operations

**Answer: B**

## Question: 959

Which of the following is MOST important for an IS auditor to consider when evaluating a Software as a Service (SaaS) arrangement?

A. Physical security
B. Software availability
C. otal cost of ownership
D. Frequency of software updates

**Answer: B**

## Question: 960

Which of the following would BEST enable effective IT resource management?

A. Automating business processes
B. Establishing business priorities
C. Outsourcing IT processes and activities
D. Assessing the risk associated with IT resources

**Answer: B**

## Question: 961

When planning an application audit, it is MOST important to evaluate risk factors by interviewing:

A. process owners
B. application owners
C. IT management
D. application users

**Answer: A**

## Question: 962

What should an IS auditor do when informed that some recommendations cannot be implemented due to financial constraints?

A. Suggest management identify cost-effective alternatives.
B. Insist the recommendations be implemented.
C. Agree to waive the recommendations.
D. Document management's response in the working papers.

**Answer: A**

## Question: 963

Of the following procedures for testing a disaster recovery plan (DRP), which should be used MOST frequently?

A. Unannounced shutdown of the primary computing facility
B. Testing at a secondary site using offsite data backups
C. Preplanned shutdown of the computing facility during an off-peak period
D. Review of documented backup and recovery procedures

**Answer: D**

## Question: 964

An IS auditor finds that a mortgage origination team receives customer mortgage applications via a shared repository. Which of the following test procedures is the BEST way to assess whether there are adequate privacy controls over this process?

A. Validate that data is entered accurately and timely.
B. Validate whether complex passwords are required.
C. Validate whether the encryption is compliant with the organization's requirements.
D. Validate whether documents are deleted according to data retention procedures.

**Answer: C**

## Question: 965

A company is using a software developer for a project. At which of the following points should the software quality assurance (QA) plan be developed?

A. Prior to acceptance testing
B. During the feasibility phase
C. As part of software definition
D. As part of the design phase

**Answer: C**

## Question: 966

An IS auditor finds that periodic reviews of read-only users for a reporting system are not being performed. Which of the following should be the IS auditor's NEXT course of action?

A. Report this control process weakness to senior management
B. Obtain a verbal confirmation from IT for this exemption.
C. Review the list of end-users and evaluate for authorization.
D. Verify managements approval for this exemption.

**Answer: C**

## Question: 967

During an audit of an organization's financial statements, an IS auditor finds that the IT general controls are deficient. What should the IS auditor recommend?

A. Increase the substantive testing of the financial balances.
B. Place greater reliance on the framework of control.

C. Place greater reliance on the application controls.
D. Increase the compliance testing of the application controls.

**Answer: D**

## Question: 968

Which of the following is MOST important for an IS auditor to consider when determining an appropriate sample size in situations where selecting the entire population is not feasible?

A. Tolerable error
B. Data integrity
C. Accessibility of the data
D. Responsiveness of the auditee

**Answer: A**

## Question: 969

To ensure the integrity of a recovered database, which of the following would be MOST useful?

A. Database defragmentation tools
B. Application transaction logs
C. A copy of the data dictionary
D. Before-and-after transaction images

**Answer: D**

## Question: 970

An IS auditor has been asked to audit the proposed acquisition of new computer hardware. The auditor's PRIMARY concern is that:

A. the implementation plan meets user requirements.
B. a clear business case has been established,
C. a full visible audit trail will be included
D. the new hardware meets established security standards.

**Answer: B**

## Question: 971

Which of the following activities is MOST important in determining whether a test of a disaster recovery plan (DRP) has been successful?
Analyzing whether predetermined test objectives were met

A. Evaluating participation by key personnel
B. Testing with offsite backup files
C. Testing at the backup data center

**Answer: A**

## Question: 972

Which of the following is the BEST reason to perform root cause analysis after a critical server failure?

A. To enable appropriate corrective measures
B. To enable timely follow-up audits
C. To enable the gathering of system availability data
D. To enable the optimization of IT investments

**Answer: A**

## Question: 973

Which of the following roles combined with the role of a database administrator (DBA) will create a segregation of duties conflict?

A. Security administrator
B. Application end user
C. Quality assurance
D. Systems analyst

**Answer: B**

## Question: 974

During an audit, the client learns that the IS auditor has recently completed a similar security review at a competitor. The client inquires about the competitor's audit results. What is the BEST way for the auditor to address this inquiry?

A. Explain that it would be inappropriate to discuss the results of another audit client
B. Escalate the question to the audit manager for further action.
C. Discuss the results of the audit omitting specifics related to names and products.
D. Obtain permission from the competitor to use the audit results as examples for future clients.

**Answer: A**

## Question: 975

Which of the following is MOST important for an IS auditor to verify when reviewing an organization's information security practices following the adoption of a bring your own device (8YOD) program?

A. Security policies have been updated to include BYOD.
B. Only applications approved by information security may be installed on devices.
C. The expected benefits of adopting the BYOD program have been realized.
D. Remote wipe is enabled for devices allowed by BYOD.

**Answer: A**

## Question: 976

Which of the following is the MOST important benefit of involving IS audit when implementing governance of enterprise IT?

A. Identifying relevant roles for an enterprise IT governance framework
B. Verifying that legal, regulatory and contractual requirements are being met
C. Providing independent and objective feedback to facilitate improvement of IT processes
D. Making decisions regarding risk response and monitoring of residual risk

**Answer: C**

## Question: 977

Which of the following procedures should be implemented prior to disposing of surplus computer equipment to employees?

A. Overwrite the hard drive with random data.
B. Use operating system commands to delete all files from the hard drive.
C. Use application delete commands to remove files.
D. Have the employee receiving the machine sign a nondisclosure agreement.

**Answer: A**

## Question: 978

Which of the following BEST demonstrates to an IS auditor that an organization has implemented effective risk management processes?

A. Critical business assets have additional controls.
B. The risk register is reviewed periodically.
C. A business impact analysis (BIA) has been completed.
D. The inventory of IT assets includes asset classification.

**Answer: A**

## Question: 979

A development team has designed a new application and incorporated best practices for secure coding. Prior to launch, which of the following is the IS auditor's BEST recommendation to mitigate the associated security risk?

A. Integration testing
B. Unit testing
C. Penetration testing
D. User acceptance testing

**Answer: C**

## Question: 980

Which of the following activities is MOST important to consider when conducting IS audit planning?

A. Audit scheduling is based on skill set of audit team.
B. Resources are allocated to areas of high risk.
C. The audit committee agrees on risk rankings.
D. Results from previous audits are reviewed.

**Answer: B**

## Question: 981

Which of the following is the BEST method for uncovering shadow IT within an organization?

A. Analyze help desk tickets.
B. Review secondary approval thresholds.
C. Use a cloud access security broker (CASB).
D. Review business processes.

**Answer: D**

## Question: 982

An organization has implemented a distributed security administration system to replace the previous centralized one. The IS auditor's GREATEST concern should be that:

A. security procedures may be inadequate to support the change.
B. a distributed security system is inherently a weak security system
C. ,the new system will require additional training
D. end-user acceptance of the new system is likely to be difficult to obtain.

**Answer: B**

## Question: 983

IT service engineers at a large organization are unable to effectively prioritize system-generated alerts from hundreds of applications running across multiple servers and databases. As a result many alerts are often ignored, leading to major problems including downtime. Which of the following is the BEST IS audit recommendation to address this situation?

A. Develop a classification scheme that prioritizes alerts according to potential business impact.
B. Group alerts from related systems and immediately escalate to the application owner.
C. Implement a threshold management system that prioritizes alerts over a certain age.
D. Prioritize alerts from legacy applications that may require remote support from external vendors.

**Answer: A**

## Question: 984

An organization's current end-user computing practices include the use of a spreadsheet for financial statements. Which of the following is the GREATEST concern?

A. Operational procedures have not been reviewed in the current fiscal year
B. The spreadsheet is not maintained by IT.

C. The spreadsheet contains numerous macros.
D. Formulas are not protected against unintended changes.

**Answer: D**

## Question: 985

An organization recently experienced a phishing attack that resulted in a breach of confidential information. Which of the following would be MOST relevant for an IS auditor to review when determining the root cause of the incident?

A. Email configurations
B. Browser configurations
C. Simple mail transfer protocol (SMTP) logging
D. Audit logging

**Answer: C**

## Question: 986

Which of the following procedures should an IS auditor complete FIRST when evaluating the adequacy of IT key performance indicators (KPIs)?

A. Validate the KPI thresholds.
B. Independently calculate the accuracy of the KPIs.
C. Review KPIs that indicate poor IT performance.
D. Determine whether the KPIs support IT objectives.

**Answer: D**

## Question: 987

Which of the following is the MOST effective control to minimize the risk of cross-site scripting (XSS)?

A. Periodic vulnerability assessments
B. Web firewall policy
C. Secure coding practices
D. Network intrusion prevention system

**Answer: C**

## Question: 988

An organization is replacing its financial processing system. To help ensure that transactions in the new system are processed accurately, which of the following is MOST appropriate?

A. Document and test internal controls over the conversion.
B. Compare year-to-date balances between the systems.
C. Review data file conversion procedures.
D. Reconcile results of parallel processing.

**Answer: D**

## Question: 989

At what point in software development should the user acceptance test plan be prepared?

A. Feasibility study
B. Transfer into production
C. Requirements definition
D. Implementation planning

**Answer: C**

## Question: 990

During an audit of a data center, an IS auditor's BEST way to gain an understanding of physical security controls is to:

A. contact the alarm vendor and identify where alarms are installed in the data center
B. review the data center's physical security procedures.
C. take a tour of the facility and identify physical security controls.
D. obtain the engineering plans for the building and identify points of entry.

**Answer: C**

## Question: 991

An IS auditor plans to review all access attempts to a video-monitored and proximity card-controlled communications room. Which of the following would be MOST useful to the auditor?

A. Manual sign-in and sign-out log
B. Security incident log
C. Alarm system with CCTV
D. System electronic log

**Answer: B**

## Question: 992

Which of the following is the BEST method for converting a file into a format suitable for data analysis in a forensic investigation?

A. Imaging
B. Extraction
C. Data acquisition
D. Normalization

**Answer: A**

## Question: 993

An IS auditor observes an organization is performing data backup and restoration testing on an ad hoc basis without a defined process. What is the MOST likely result of a data disruption event?

A. Increased loss impact
B. Increased likelihood of future risk events
C. Decreased data integrity
D. Decreased data confidentiality

**Answer: A**

## Question: 994

Which of the following management decisions presents the GREATEST risk associated with data leakage?

A. Security awareness training is not provided to staff.
B. There is no requirement for desktops to be encrypted.
C. Security policies have not been updated in the past year
D. Staff are allowed to work remotely.

**Answer: D**

## Question: 995

In the IT department where segregation of duties is not feasible due to a limited number of resources, a team member is performing the functions of computer operator and reviewer of application logs. Which of the following would be the IS auditor's BEST recommendation?

A. Prevent the operator from performing application development activities.
B. Restrict the computer operator's access to the production environment
C. Assign an independent second reviewer to verify the application logs.
D. Develop procedures to verify that the application logs are not modified.

**Answer: D**

## Question: 996

Which of the following is MOST important for the IS auditor to verify when reviewing the development process of a security policy?

A. Evidence of active involvement of key stakeholders
B. Evidence of management approval
C. Identification of the control framework
D. Output from the enterprise's risk management system

**Answer: D**

## Question: 997

A design company has multiple name and address files for its customers in several of its independent systems. Which of the following is the BEST control to ensure that the customer name and address agree across all files?

A. Matching of records and review of exception reports
B. Use of authorized master file change forms
C. Periodic review of each master file by management
D. Use of hash totals on customer records

**Answer: B**

## Question: 998

The BEST method an organization can employ to align its business continuity plan (BCP) and disaster recovery plan (DRP) with core business needs is to:

A. include BCP and disaster recovery plan responsibilities as a part of new employee training,
B. execute periodic walk-throughs of the plans.
C. update the business impact analysis (BIA) for significant business changes.
D. outsource the maintenance of the BCP and disaster recovery plan to a third party.

**Answer: C**

## Question: 999

The lack of which of the following represents the GREATEST risk to the quality of developed software?

A. An enterprise architecture
B. Periodic internal audits
C. Load testing
D. Code reviews

**Answer: D**

## Question: 1000

An organization has decided to migrate payroll processing to a new platform hosted by a third party in a different country. Which of the following is MOST important for the IS auditor to consider?

A. The service provider's compliance with financial regulations
B. Storage costs charged by the service provider
C. Whether the contract contains a right-to-terminate clause
D. The service provider's compliance with privacy regulations

**Answer: D**

## Question: 1001

At a project steering committee meeting, it is stated that adding controls to business processes undergoing re-engineering is an unnecessary cost. The IS auditor's BEST response is that the actual control overhead for a business process is:

A. usually difficult to ascertain but is justifiable, because controls are essential to doing business.
B. the responsibility of the project manager, and the cost should have been included in the budget.
C. usually considerable, but the benefits of good controls always exceed the cost,
D. usually less than the potential cost of failure caused by lack of controls.

**Answer: C**

## Question: 1002

Nonrepudiation of the client for e-commerce transactions is accomplished through which of the following control mechanisms?

A. Public key infrastructure (PKI)
B. Internet protocol (IP) address verification
C. Password security
D. Secure Sockets Layer (SSL)

**Answer: D**

## Question: 1003

Which of the following is the MOST important reason to periodically review data that has already been classified?

A. Older data may need to be archived on removable media.
B. Additional data may have been added to the inventory.
C. The classification nomenclature has changed.
D. The associated risk may change over time.

**Answer: D**

## Question: 1004

A sales representative is reviewing the organization's feedback blog and gets redirected to a site that sells illegal prescription drugs. The blog site is MOST likely susceptible to which of the following types of attacks?

A. Directory harvesting
B. Phishing attack
C. Cross-site scripting
D. SQL injection

**Answer: C**

## Question: 1005

Which of the following BEST indicates the effectiveness of an organization's risk management program?

A. Overall risk is quantified.
B. Residual risk is minimized.
C. Inherent risk is eliminated.
D. Control risk is minimized.

**Answer: B**

## Question: 1006

Which of the following controls should be implemented to BEST minimize system downtime for maintenance?

A. Virtualization
B. Nightly full backups
C. Clustering
D. Warm site

**Answer: C**

## Question: 1007

An enterprise receiving email should have procedures to control:

A. insufficient connectivity,
B. outdated protocols,
C. insufficient end-points.
D. unsolicited executable code.

**Answer: D**

## Question: 1008

Which of the following controls would BEST decrease the exposure if a password is compromised?

A. Password changes are forced periodically.
B. Passwords are encrypted.
C. Passwords are masked.
D. Passwords have format restrictions.

**Answer: B**

## Question: 1009

Which of the following activities would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA)?

A. Partially completing the CSA
B. Developing the CSA questionnaire
C. Developing the remediation plan
D. Implementing the remediation plan

**Answer: D**

## Question: 1010

An existing system is being replaced with a new application package. User acceptance testing (UAT) should ensure that:

A. the new system functions as expected.
B. data from the old system has been converted correctly
C. there is a business need for the new system.
D. the new system is better than the old system.

**Answer: A**

## Question: 1011

In a decentralized organization, the selection and purchase of IS products is acceptable as long as which of the following conditions exists?

A. Acquired items are consistent with the organization's short- and long-term IS strategy plans.
B. Managers undertake a full cost-benefit analysis before deciding what to purchase.
C. Various offices are independent and exchange data on an occasional basis.
D. The same operating system is used throughout the organization.

**Answer: A**

## Question: 1012

Which of the following is the MOST effective way to assess whether an outsourcer's controls are following the service level agreement (SLA)?

A. Perform a review of penalty clauses for non-performance.
B. Review an internal audit report from the outsourcer's auditor.
C. Review the outsourcer's monthly service reports.
D. Perform an onsite review of the outsourcer.

**Answer: D**

## Question: 1013

Which of the following is the MOST effective control to ensure electronic records beyond their retention periods are deleted from IT systems?

A. Build in system logic to trigger data deletion at predefined times.
B. Perform a sample check of current data against the retention schedule.
C. Review the record retention register regularly to initiate data deletion.
D. Execute all data deletions at a predefined month during the year.

**Answer: A**

## Question: 1014

Which of the following would help determine the maturity of an information security awareness program?

A. A simulated social engineering test
B. A gap assessment against an established model
C. A network vulnerability assessment
D. A review of the annual penetration test results

**Answer: A**

## Question: 1015

Which of the following is the PRIMARY benefit of including IT management and staff when conducting control self-assessments (CSAs) within an organization?

A. It reduces the workload of external and internal auditors.
B. It improves the efficiency of business and IT operational processes.
C. It increases buy-in for more stringent controls.
D. It helps to identify risk to the business.

**Answer: B**

## Question: 1016

A government organization uses standard Wi-Fi Protected Access 2 (WPA2) to protect confidential information transmitted to a file server. Which of the following is the IS auditor's BEST recommendation to further strengthen security?

A. Certificate-based authentication
B. Network address translation (NAT)
C. Service set identifier (SSID) masking
D. Media access control (MAC) address filtering

**Answer: A**

## Question: 1017

Management has agreed to perform multiple remediation actions in response to an audit issue, including the implementation of a new control. Which of the following is the BEST time for an IS auditor to perform an audit follow-up of this issue?

A. After management has completed the required actions
B. When audit resources are available
C. After the new control has been in place for one year
D. When management resources are available

**Answer: A**

## Question: 1018

A multinational company wants to establish a mandatory global standard for information security including data protection and privacy. Which of the following should be the GREATEST concern to an IS auditor?

A. Increased organizational effort without any tangible benefit
B. Lack of adoption by organized labor groups in all affected countries
C. Inconsistent roll-out of the standard across all countries
D. Noncompliance with local laws in the affected countries

**Answer: D**

## Question: 1019

During an ERP post-implementation review, it was noted that operating costs have been significantly higher than anticipated. Which of the following should the organization have done to detect this issue?

A. Monitored financial key performance indicators (KPIs)
B. Performed an analysis of system usage
C. Conducted periodic user satisfaction surveys
D. Updated the project charter as major changes occurred

**Answer: A**

## Question: 1020

Which of the following IS audit recommendations would BEST help to ensure appropriate mitigation will occur on control weaknesses identified during an audit?

A. Implement software to input the action points from the IS audit.
B. Report on progress to the audit committee.
C. Assign actions to responsible personnel and follow up.
D. Perform a cost-benefit analysis on remediation strategy.

**Answer: C**

## Question: 1021

In an environment where most IT services have been outsourced, continuity planning is BEST controlled by:

A. IT management,
B. continuity planning specialists.
C. business management.
D. outsourced service provider management

**Answer: C**

## Question: 1022

An IS auditor finds that an organization's data loss prevention (DLP) system is configured to use vendor default settings to identify violations. The auditor's MAIN concern should be that:

A. violation reports may not be reviewed in a timely manner.
B. violations may not be categorized according to the organization's risk profile.
C. violation reports may not be retained according to the organization's risk profile.
D. a significant number of false positive violations may be reported.

**Answer: B**

## Question: 1023

A maturity model is useful in the assessment of IT service management because it:

A. indicates the service levels required for the business area,
B. specifies the mechanism needed to achieve defined service levels.
C. provides a benchmark for process improvement.
D. defines the level of control required to meet business needs.

**Answer: C**

## Question: 1024

Which of the following methods should be used to effectively erase sensitive data from portable storage devices that are to be reused?

A. Using media sanitization software
B. Exposing the portable device to a magnetic field
C. Formatting the portable device
D. Overwriting the sensitive data

**Answer: B**

## Question: 1025

Which of the following should be of GREATEST concern to an IS auditor when evaluating a new system's production readiness?

A. Projected benefits have not been realized.
B. Functional design documentation is not complete.
C. Functional requirements have not been met.
D. A system defect was found during user acceptance testing.

**Answer: C**

## Question: 1026

Which of the following is MOST important for an IS auditor to determine when evaluating a database for privacy-related risks?

A. Whether copies of production data are masked
B. Whether all database tables are normalized
C. Whether the integrity of the data dictionary is maintained
D. Whether data import and export procedures are approved

**Answer: A**

## Question: 1027

What is an IS auditor's BEST recommendation to management if a review of the incident management process finds multiple instances of incident tickets remaining open for an unusually long time?

A. Implement reporting of key performance indicators (KPIs) for ticket closure.
B. Manually review the identified tickets and mark as closed in the system.
C. Increase the number of help desk staff to enable faster ticket closure.
D. Configure the system to automatically close tickets after a defined period.

**Answer: A**

## Question: 1028

Which of the following is the MOST appropriate action to formalize IT governance in an organization?

A. Establishing an IT steering committee
B. Evaluating the IT strategy
C. Modifying IT goals and strategy
D. Implementing risk management

**Answer: A**

## Question: 1029

An internal review reveals an out-of-support human resources system. Which of the following is MOST important to determine when evaluating the associated risk?

A. The number of people accessing the out-of-support system
B. Frequency of outages associated with the out-of-support system
C. Timeline to replace the out-of-support system
D. Exposure of the out-of-support system outside of the network

**Answer: D**

## Question: 1030

An IS audit reveals that an organization is not proactively addressing known vulnerabilities. Which of the following should the IS auditor recommend the organization do FIRST?

A. Ensure the intrusion prevention system (IPS) is effective.
B. Verify the disaster recovery plan (DRP) has been tested.
C. Confirm the incident response team understands the issue.
D. Assess the security risks to the business.

**Answer: D**

## Question: 1031

Which of the following is the PRIMARY benefit of using an integrated audit approach?

A. The avoidance of duplicated work and redundant recommendations
B. A holistic perspective of overall risk and a better understanding of controls
C. Enhanced allocation of resources and reduced audit costs
D. Higher acceptance of the findings from the audited business areas

**Answer: B**

## Question: 1032

During a database audit, an IS auditor notes frequent problems due to the growing size of the order tables. Which of the following is the BEST recommendation in this situation?

A. Periodically delete completed orders.
B. Migrate to a different database management system.
C. Develop an archiving approach.
D. Build more table indices.

**Answer: C**

## Question: 1033

Which of the following is the PRIMARY purpose of documenting and approving an information security policy?

A. To mitigate the organization's information security risk to an acceptable level
B. To communicate management's intent for securing the organization's information assets
C. To determine the best approach for implementing information security within the organization
D. To ensure awareness of disciplinary procedures for security breaches by authorized users

**Answer: B**

## Question: 1034

Which of the following is the PRIMARY advantage of the IT portfolio management approach over the balanced scorecard approach when managing IT investments?

A. Incorporation of organizational strategy in investment decisions
B. The influence of qualitative factors on investment decisions
C. Use of the organization's risk appetite in investment decisions
D. Agility in adjusting investment decisions

**Answer: A**

## Question: 1035

Which of the following is MOST important to include in a business continuity plan (BCP)?

A. Documentation of critical systems
B. Documentation of data center floor plans
C. Vendor contact information
D. Backup site location information

**Answer: D**

## Question: 1036

Capacity management enables organizations to:

A. establish the capacity of network communication links.
B. forecast technology trends.
C. determine business transaction volumes.
D. identify the extent to which components need to be upgraded.

**Answer: C**

## Question: 1037

Loading of illegal software packages onto a network by an employee is MOST effectively detected by:

A. maintaining current antivirus software
B. logging of activity on network drives
C. diskless workstations
D. regular scanning of hard drives

**Answer: B**

## Question: 1038

Which of the following BEST determines if a batch update job was completed?

A. Reviewing the job log
B. Obtaining process owner confirmation
C. Testing a sample of transactions
D. Reviewing a copy of the script

**Answer: C**

## Question: 1039

Which of the following should be an IS auditor's FIRST action when assessing the risk associated with unstructured data?

A. Identify appropriate tools for data classification.
B. Identify repositories of unstructured data.
C. Implement user access controls to unstructured data.
D. Implement strong encryption for unstructured data.

**Answer: A**

## Question: 1040

Which of the following access rights in the production environment should be granted to a developer to maintain segregation of duties?

A. System administration
B. Emergency support
C. Database administration
D. IT operations

**Answer: B**

## Question: 1041

Which of the following audit procedures would be MOST conclusive in evaluating the effectiveness of an e-commerce application system's edit routine?

A. Review of program documentation
B. Use of test transactions
C. Interviews with knowledgeable users
D. Review of source code

**Answer: D**

## Question: 1042

Which of the following would BEST prevent data from being orphaned?

A. Input validation checks
B. Table partitioning
C. Table indexes
D. Referential integrity

**Answer: D**

## Question: 1043

An organization using instant messaging to communicate with customers can prevent legitimate customers from being impersonated by:

A. using call monitoring
B. logging conversations.
C. authenticating users before conversations are initiated
D. using firewalls to limit network traffic to authorized ports.

**Answer: C**

# Thank You for Trying Our Product

**Discount Coupon Code:**
**EXAMSBOOST10**

For More Information – **Visit link below:**

**http://www.examsboost.com/**




## FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer