CISA Dumps

Isaca CISA

https://www.certleader.com/CISA-dumps.html

NEW QUESTION 1
- (Topic 1)
Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?

A. Field checks
B. Control totals
C. Reasonableness checks
D. A before-and-after maintenance report

Answer: D

Explanation:

A before-and-after maintenance report is the best answer because a visual review would provide the most positive verification that updating was proper.

NEW QUESTION 2
- (Topic 1)
Which of the following is a dynamic analysis tool for the purpose of testing software modules?

A. Blackbox test
B. Desk checking
C. Structured walk-through
D. Design and code

Answer: A

Explanation:

A blackbox test is a dynamic analysis tool for testing software modules. During the testing of software modules a blackbox test works first in a cohesive manner as one single unit/entity, consisting of numerous modules and second, with the user data that flows across software modules. In some cases, this even drives the software behavior.

NEW QUESTION 3
- (Topic 1)
Which of the following is MOST likely to result from a business process reengineering (BPR) project?

A. An increased number of people using technology
B. Significant cost savings, through a reduction in the complexity of information technology
C. A weaker organizational structures and less accountability
D. Increased information protection (IP) risk will increase

Answer: A

Explanation:

A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern. Incorrect answers:
B. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this areA.
D. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

NEW QUESTION 4
- (Topic 1)
Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

A. Router
B. Bridge
C. Repeater
D. Gateway

Answer: B

Explanation:

A bridge connects two separate networks to form a logical network (e.g., joining an ethernet and token network) and has the storage capacity to store frames and act as a storage and forward device. Bridges operate at the OSI data link layer by examining the media access control header of a data packet.

NEW QUESTION 5
- (Topic 1)
A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

A. dials back to the user machine based on the user id and password using a telephone number from its databas
B. dials back to the user machine based on the user id and password using a telephone number provided by the user during this connectio
C. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using its databas
D. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using the sender's databas

Answer: A

Explanation:

A call-back system in a net centric environment would mean that a user with an id and password calls a remote server through a dial-up line first, and then the server disconnects and dials back to the user machine based on the user id and password using a telephone number from its database. Although the server can depend upon its own database, it cannot know the authenticity of the dialer when the user dials again. The server cannot depend upon the sender's database to dial back as the same could be manipulated.

NEW QUESTION 6
- (Topic 1)
An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

A. cold sit
B. warm sit
C. dial-up sit
D. duplicate processing facilit

Answer: A

Explanation:

A cold site is ready to receive equipment but does not offer any components at the site in advance of the need.

NEW QUESTION 7
- (Topic 1)
The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

A. testing stag
B. evaluation stag
C. maintenance stag
D. early stages of plannin

Answer: D

Explanation:

Company.com in the early stages of a BCP will incur the most significant level of program development effort, which will level out as the BCP moves into maintenance, testing and evaluation stages. It is during the planning stage that an IS auditor will play an important role in obtaining senior management's commitment to resources and assignment of BCP responsibilities.

NEW QUESTION 8
- (Topic 1)
Which of the following network configuration options contains a direct link between any two host machines?

A. Bus
B. Ring
C. Star
D. Completely connected (mesh)

Answer: D

Explanation:

A completely connected mesh configuration creates a direct link between any two host machines.

NEW QUESTION 9
- (Topic 1)
Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

A. A substantive test of program library controls
B. A compliance test of program library controls
C. A compliance test of the program compiler controls
D. A substantive test of the program compiler controls

Answer: B

Explanation:

A compliance test determines if controls are operating as designed and are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned whether program library controls are working properly, the IS auditor might select a sample of programs to determine if the source and object versions are the same. In other words, the broad objective of any compliance test is to provide auditors with reasonable assurance that a particular control on which the auditor plans to rely is operating as the auditor perceived it in the preliminary evaluation.

NEW QUESTION 10
- (Topic 1)
A data administrator is responsible for:

A. maintaining database system softwar
B. defining data elements, data names and their relationshi
C. developing physical database structure
D. developing data dictionary system softwar

Answer: B

Explanation:

A data administrator is responsible for defining data elements, data names and their relationship. Choices A, C and D are functions of a database administrator (DBA)

NEW QUESTION 10
- (Topic 1)
A database administrator is responsible for:

A. defining data ownershi
B. establishing operational standards for the data dictionar
C. creating the logical and physical databas
D. establishing ground rules for ensuring data integrity and securit

Answer: C

Explanation:

A database administrator is responsible for creating and controlling the logical and physical database. Defining data ownership resides with the head of the user department or top management if the data is common to the organization. IS management and the data administrator are responsible for establishing operational standards for the data dictionary. Establishing ground rules for ensuring data integrity and security in line with the corporate security policy is a function of the security administrator.

NEW QUESTION 12
- (Topic 1)
Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

A. Gateway
B. Protocol converter
C. Front-end communication processor
D. Concentrator/multiplexor

Answer: A

Explanation:

A gateway performs the job of translating e-mail formats from one network to another so messages can make their way through all the networks.

NEW QUESTION 13
- (Topic 1)
Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

A. Specific developments only
B. Business requirements only
C. All phases of the installation must be documented
D. No need to develop a customer specific documentation

Answer: C

Explanation:

A global enterprise product reengineering (EPR) software package can be applied to a business to replace, simplify and improve the quality of IS processing. Documentation is intended to help understand how, why and which solutions that have been selected and implemented, and therefore must be specific to the project. Documentation is also intended to support quality assurance and must be comprehensive.

NEW QUESTION 15
- (Topic 1)
A hub is a device that connects:

A. two LANs using different protocol
B. a LAN with a WA
C. a LAN with a metropolitan area network (MAN).
D. two segments of a single LA

Answer: D

Explanation:

A hub is a device that connects two segments of a single LAN. A hub is a repeater. It provides transparent connectivity to users on all segments of the same LAN. It is a level 1 device.

NEW QUESTION 20
- (Topic 1)
A LAN administrator normally would be restricted from:

A. having end-user responsibilitie
B. reporting to the end-user manage
C. having programming responsibilitie
D. being responsible for LAN security administratio

Answer: C

Explanation:

A LAN administrator should not have programming responsibilities but may have end- user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator also may be responsible for security administration over the LAN.

NEW QUESTION 25
- (Topic 1)
Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

A. A neural network
B. Database management software
C. Management information systems
D. Computer assisted audit techniques

Answer: A

Explanation:

A neural network will monitor and learn patterns, reporting exceptions for investigation.

NEW QUESTION 28
- (Topic 1)
Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

A. Paper test
B. Post test
C. Preparedness test
D. Walk-through

Answer: C

Explanation:

A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments.

NEW QUESTION 30
- (Topic 1)
The IS auditor learns that when equipment was brought into the data center by a vendor, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?

A. Relocate the shut off switc
B. Install protective cover
C. Escort visitor
D. Log environmental failure

Answer: B

Explanation:

A protective cover over the switch would allow it to be accessible and visible, but would prevent accidental activation.

NEW QUESTION 33
- (Topic 1)
What is the primary objective of a control self-assessment (CSA) program?

A. Enhancement of the audit responsibility
B. Elimination of the audit responsibility
C. Replacement of the audit responsibility
D. Integrity of the audit responsibility

Answer: A

Explanation:
Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

NEW QUESTION 38
- (Topic 1)
IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

A. True
B. False

Answer: A

Explanation:
IS auditors are most likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. Think of it this way: If any reliance is placed on internal controls, that reliance must be validated through compliance testing. High control risk results in little reliance on internal controls, which results in additional substantive testing.

NEW QUESTION 42
- (Topic 1)
How does the process of systems auditing benefit from using a risk-based approach to audit planning?

A. Controls testing starts earlie
B. Auditing resources are allocated to the areas of highest concer
C. Auditing risk is reduce
D. Controls testing is more thoroug

Answer: B

Explanation:
Allocation of auditing resources to the areas of highest concern is a benefit of a risk-based approach to audit planning.

NEW QUESTION 45
- (Topic 1)
The use of statistical sampling procedures helps minimize:

A. Detection risk
B. Business risk
C. Controls risk
D. Compliance risk

Answer: A

Explanation:
The use of statistical sampling procedures helps minimize detection risk.

NEW QUESTION 47
- (Topic 1)
Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

A. True
B. False

Answer: A

Explanation:
Proper segregation of duties prohibits a system analyst from performing quality-assurance functions.

NEW QUESTION 51
- (Topic 1)
Batch control reconciliation is a _____ (fill in the blank) control for mitigating risk of inadequate segregation of duties.

A. Detective
B. Corrective
C. Preventative
D. Compensatory

Answer: D

Explanation:
Batch control reconciliations is a compensatory control for mitigating risk of inadequate segregation of duties.

NEW QUESTION 53
- (Topic 1)
If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

A. IT cannot be implemented if senior management is not committed to strategic plannin
B. More likel
C. Less likel
D. Strategic planning does not affect the success of a company's implementation of I

Answer: C

Explanation:
A company's implementation of IT will be less likely to succeed if senior management is not committed to strategic planning.

NEW QUESTION 58
- (Topic 1)
What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?

A. Nonconnection-oriented protocols
B. Connection-oriented protocols
C. Session-oriented protocols
D. Nonsession-oriented protocols

Answer: B

Explanation:
The transport layer of the TCP/IP protocol suite provides for connection-oriented protocols to ensure reliable communication.

NEW QUESTION 60
- (Topic 1)
How is the time required for transaction processing review usually affected by properly implemented Electronic Data Interface (EDI)?

A. EDI usually decreases the time necessary for revie
B. EDI usually increases the time necessary for revie
C. Cannot be determine
D. EDI does not affect the time necessary for revie

Answer: A

Explanation:
Electronic data interface (EDI) supports intervendor communication while decreasing the time necessary for review because it is usually configured to readily identify errors requiring follow-up.

NEW QUESTION 63
- (Topic 1)
Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing. True or false?

A. True
B. False

Answer: A

Explanation:
Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing.

NEW QUESTION 67
- (Topic 1)
What is essential for the IS auditor to obtain a clear understanding of network management?

A. Security administrator access to systems
B. Systems logs of all hosts providing application services
C. A graphical map of the network topology
D. Administrator access to systems

Answer: C

Explanation:
A graphical interface to the map of the network topology is essential for the IS auditor to obtain a clear understanding of network management.

NEW QUESTION 72
- (Topic 1)
What increases encryption overhead and cost the most?

A. A long symmetric encryption key
B. A long asymmetric encryption key
C. A long Advance Encryption Standard (AES) key
D. A long Data Encryption Standard (DES) key

Answer: B

Explanation:
A long asymmetric encryption key (public key encryption) increases encryption overhead and cost. All other answers are single shared symmetric keys.

NEW QUESTION 74
- (Topic 1)
What are used as the framework for developing logical access controls?

A. Information systems security policies
B. Organizational security policies
C. Access Control Lists (ACL)
D. Organizational charts for identifying roles and responsibilities

Answer: A

Explanation:
Information systems security policies are used as the framework for developing logical access controls.

NEW QUESTION 75
- (Topic 1)
Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

A. Concurrency controls
B. Reasonableness checks
C. Time stamps
D. Referential integrity controls

Answer: C

Explanation:
Time stamps are an effective control for detecting duplicate transactions such as payments made or received.

NEW QUESTION 77
- (Topic 1)
What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?

A. A combination of public-key cryptography and digital certificates and two-factor authentication
B. A combination of public-key cryptography and two-factor authentication
C. A combination of public-key cryptography and digital certificates
D. A combination of digital certificates and two-factor authentication

Answer: C

Explanation:
PKI uses a combination of public-key cryptography and digital certificates to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions.

NEW QUESTION 81
- (Topic 1)
Regarding digital signature implementation, which of the following answers is correct?

A. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's private ke
B. Upon receiving the data, the recipient can decrypt the data using the sender's public ke
C. A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public ke
D. Upon receiving the data, the recipient can decrypt the data using the recipient's public ke
E. A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value or message digest from the entire message content
F. Upon receiving the data, the recipient can independently create i
G. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public ke
H. Upon receiving the data, the recipient can decrypt the data using the recipient's private ke

Answer: C

Explanation:
A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value, or message digest, from the entire message contents. Upon receiving the data, the recipient can independently create its own message digest from the data for comparison and data integrity validation. Public and private are used to enforce confidentiality. Hashing algorithms are used to enforce integrity.

NEW QUESTION 84
- (Topic 1)
What are often the primary safeguards for systems software and data?

A. Administrative access controls
B. Logical access controls
C. Physical access controls
D. Detective access controls

Answer: B

Explanation:
Logical access controls are often the primary safeguards for systems software and datA.
Which of the following is often used as a detection and deterrent control against Internet
attacks? A. Honeypots B. CCTV C. VPN D. VLAN Answer: A Honeypots are often used as a detection and deterrent control against Internet attacks.

NEW QUESTION 89
- (Topic 1)
Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

A. A monitored double-doorway entry system
B. A monitored turnstile entry system
C. A monitored doorway entry system
D. A one-way door that does not allow exit after entry

Answer: A

Explanation:
A monitored double-doorway entry system, also referred to as a mantrap or deadman door, is used as a deterrent control for the vulnerability of piggybacking.

NEW QUESTION 94
- (Topic 1)
Which of the following provides the strongest authentication for physical access control?

A. Sign-in logs
B. Dynamic passwords
C. Key verification
D. Biometrics

Answer: D

Explanation:
Biometrics can be used to provide excellent physical access control.

NEW QUESTION 98
- (Topic 1)
What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources? Choose the BEST answer.

A. OSI Layer 2 switches with packet filtering enabled
B. Virtual Private Networks
C. Access Control Lists (ACL)
D. Point-to-Point Tunneling Protocol

Answer: C

Explanation:
ISPs can use access control lists to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources.

NEW QUESTION 102
- (Topic 1)
What is the key distinction between encryption and hashing algorithms?

A. Hashing algorithms ensure data confidentialit
B. Hashing algorithms are irreversibl
C. Encryption algorithms ensure data integrit
D. Encryption algorithms are not irreversibl

Answer: B

Explanation:
A key distinction between encryption and hashing algorithms is that hashing
algorithms are irreversible.

NEW QUESTION 107
- (Topic 1)
Which of the following is used to evaluate biometric access controls?

A. FAR
B. EER
C. ERR
D. FRR

Answer: B

Explanation:
When evaluating biometric access controls, a low equal error rate (EER) is preferred. EER is also called the crossover error rate (CER).

NEW QUESTION 109
- (Topic 1)
Establishing data ownership is an important first step for which of the following processes? Choose the BEST answer.

A. Assigning user access privileges
B. Developing organizational security policies
C. Creating roles and responsibilities
D. Classifying data

Answer: D

Explanation:
To properly implement data classification, establishing data ownership is an important first step.

NEW QUESTION 113
- (Topic 1)
Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

A. End-user involvement
B. Senior management involvement
C. Security administration involvement
D. IS auditing involvement

Answer: A

Explanation:
End-user involvement is critical during the business impact assessment phase of business continuity planning.

NEW QUESTION 116
- (Topic 1)
What type of BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness?

A. Paper
B. Preparedness
C. Walk-through
D. Parallel

Answer: B

Explanation:
Of the three major types of BCP tests (paper, walk-through, and preparedness), only the preparedness test uses actual resources to simulate a system crash and validate the plan's effectiveness.

NEW QUESTION 117
- (Topic 1)
Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

A. Parallel
B. Preparedness
C. Walk-thorough
D. Paper

Answer: C

Explanation:
Of the three major types of BCP tests (paper, walk-through, and preparedness), a walk-through test requires only that representatives from each operational area meet to review the plan.

NEW QUESTION 122
- (Topic 1)
Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

A. Cold site
B. Alternate site
C. Hot site
D. Warm site

Answer: A

Explanation:
Of the three major types of off-site processing facilities (hot, warm, and cold), a cold site is characterized by at least providing for electricity and HVAC. A warm site improves upon this by providing for redundant equipment and software that can be made operational within a short time.

NEW QUESTION 127
- (Topic 1)
Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive

management, such as the _____. (fill-in-the-blank)

A. Security administrator
B. Systems auditor
C. Board of directors
D. Financial auditor

Answer: C

Explanation:
Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the board of directors.

NEW QUESTION 132
- (Topic 1)
Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

A. True
B. False

Answer: A

Explanation:
Obtaining user approval of program changes is very effective for controlling application changes and maintenance.

NEW QUESTION 136
- (Topic 1)
When is regression testing used to determine whether new application changes have
introduced any errors in the remaining unchanged code?

A. In program development and change management
B. In program feasibility studies
C. In program development
D. In change management

Answer: A

Explanation:
Regression testing is used in program development and change management to determine whether new changes have introduced any errors in the remaining unchanged code.

NEW QUESTION 139
- (Topic 1)
What is a primary high-level goal for an auditor who is reviewing a system development project?

A. To ensure that programming and processing environments are segregated
B. To ensure that proper approval for the project has been obtained
C. To ensure that business objectives are achieved
D. To ensure that projects are monitored and administrated effectively

Answer: C

Explanation:
A primary high-level goal for an auditor who is reviewing a systems-development project is to ensure that business objectives are achieved. This objective guides all other systems development objectives.

NEW QUESTION 144
- (Topic 1)
Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs. True or false?

A. True
B. False

Answer: B

Explanation:
Function point analysis (FPA) provides an estimate of the size of an information system based on the number and complexity of a system's inputs, outputs, and files.

NEW QUESTION 148
- (Topic 1)
Who assumes ownership of a systems-development project and the resulting system?

A. User management
B. Project steering committee
C. IT management

D. Systems developers

Answer: A

Explanation:
User management assumes ownership of a systems-development project and the resulting system.

NEW QUESTION 153
- (Topic 1)
When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

A. True
B. False

Answer: B

Explanation:
When participating in a systems-development project, an IS auditor should also strive to ensure that adequate and complete documentation exists for all projects.

NEW QUESTION 155
- (Topic 1)
Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

A. Function Point Analysis (FPA)
B. GANTT
C. Rapid Application Development (RAD)
D. PERT

Answer: D

Explanation:
PERT is a program-evaluation review technique that considers different scenarios for planning and control projects.

NEW QUESTION 157
- (Topic 1)
What often results in project scope creep when functional requirements are not defined as well as they could be?

A. Inadequate software baselining
B. Insufficient strategic planning
C. Inaccurate resource allocation
D. Project delays

Answer: A

Explanation:
Inadequate software baselining often results in project scope creep because functional requirements are not defined as well as they could be.

NEW QUESTION 160
- (Topic 1)
Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures. True or false?

A. True
B. False

Answer: A

Explanation:
Fourth-generation languages(4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures.

NEW QUESTION 161
- (Topic 1)
_____ (fill in the blank) is/are are ultimately accountable for the functionality, reliability, and security within IT governance. Choose the BEST answer.

A. Data custodians
B. The board of directors and executive officers
C. IT security administration
D. Business unit managers

Answer: B

Explanation:
The board of directors and executive officers are ultimately accountable for the functionality, reliability, and security within IT governance.

NEW QUESTION 163
- (Topic 1)
What can be used to help identify and investigate unauthorized transactions? Choose the BEST answer.

A. Postmortem review
B. Reasonableness checks
C. Data-mining techniques
D. Expert systems

Answer: C

Explanation:
Data-mining techniques can be used to help identify and investigate unauthorized transactions.

NEW QUESTION 164
- (Topic 1)
Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

A. True
B. False

Answer: A

Explanation:
Network environments often add to the complexity of program-to-program communication, making application systems implementation and maintenance more difficult.

NEW QUESTION 168
- (Topic 1)
What must an IS auditor understand before performing an application audit? Choose the BEST answer.

A. The potential business impact of application risk
B. Application risks must first be identifie
C. Relative business processe
D. Relevant application risk

Answer: C

Explanation:
An IS auditor must first understand relative business processes before performing an application audit.

NEW QUESTION 173
- (Topic 1)
When storing data archives off-site, what must be done with the data to ensure data completeness?

A. The data must be normalize
B. The data must be validate
C. The data must be parallel-teste
D. The data must be synchronize

Answer: D

Explanation:
When storing data archives off-site, data must be synchronized to ensure data completeness.

NEW QUESTION 177
- (Topic 1)
Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

A. Redundancy check
B. Completeness check
C. Accuracy check
D. Parity check

Answer: A

Explanation:
A redundancy check can help detect transmission errors by appending especially calculated bits onto the end of each segment of datA.

NEW QUESTION 180
- (Topic 1)
An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

A. True
B. False

Answer: B

Explanation:
An intentional or unintentional disclosure of a password is not likely to be evident within control logs.

NEW QUESTION 181
- (Topic 1)
A check digit is an effective edit check to:

A. Detect data-transcription errors
B. Detect data-transposition and transcription errors
C. Detect data-transposition, transcription, and substitution errors
D. Detect data-transposition errors

Answer: B

Explanation:
A check digit is an effective edit check to detect data-transposition and transcription errors.

NEW QUESTION 183
- (Topic 1)
Parity bits are a control used to validate:

A. Data authentication
B. Data completeness
C. Data source
D. Data accuracy

Answer: B

Explanation:
Parity bits are a control used to validate data completeness.

NEW QUESTION 187
- (Topic 1)
What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

A. Document existing internal controls
B. Perform compliance testing on internal controls
C. Establish a controls-monitoring steering committee
D. Identify high-risk areas within the organization

Answer: D

Explanation:
When implementing continuous-monitoring systems, an IS auditor's first step is to identify highrisk areas within the organization.

NEW QUESTION 189
- (Topic 1)
What type of risk is associated with authorized program exits (trap doors)? Choose the BEST answer.

A. Business risk
B. Audit risk
C. Detective risk
D. Inherent risk

Answer: D

Explanation:
Inherent risk is associated with authorized program exits (trap doors).

NEW QUESTION 194
- (Topic 1)
Which of the following is best suited for searching for address field duplications?

A. Text search forensic utility software
B. Generalized audit software
C. Productivity audit software
D. Manual review

Answer: B

Explanation:
Generalized audit software can be used to search for address field duplications.

NEW QUESTION 195

- (Topic 1)
An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

A. True
B. False

Answer: A

Explanation:
It is true that an advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions.

NEW QUESTION 197
- (Topic 1)
If an IS auditor finds evidence of risk involved in not implementing proper segregation of
duties, such as having the security administrator perform an operations function, what is the auditor's primary responsibility?

A. To advise senior managemen
B. To reassign job functions to eliminate potential frau
C. To implement compensator control
D. Segregation of duties is an administrative control not considered by an IS audito

Answer: A

Explanation:
An IS auditor's primary responsibility is to advise senior management of the risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function.

NEW QUESTION 199
- (Topic 1)
Who is responsible for implementing cost-effective controls in an automated system?

A. Security policy administrators
B. Business unit management
C. Senior management
D. Board of directors

Answer: B

Explanation:
Business unit management is responsible for implementing cost-effective controls in an automated system.

NEW QUESTION 202
- (Topic 1)
Why does an IS auditor review an organization chart?

A. To optimize the responsibilities and authority of individuals
B. To control the responsibilities and authority of individuals
C. To better understand the responsibilities and authority of individuals
D. To identify project sponsors

Answer: C

Explanation:
The primary reason an IS auditor reviews an organization chart is to better understand the responsibilities and authority of individuals.

NEW QUESTION 206
- (Topic 1)
When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.

A. Ownership of the programs and files
B. A statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster
C. A statement of due care
D. Ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster

Answer: D

Explanation:
When auditing third-party service providers, an auditor should be concerned with ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster.

NEW QUESTION 208
- (Topic 1)
When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

A. Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic pla
B. Reviewing an audit client's business plan should be performed after reviewing an organization's IT strategic pla
C. Reviewing an audit client's business plan should be performed during the review of an organization's IT strategic pla
D. Reviewing an audit client's business plan should be performed without regard to an organization's IT strategic pla

Answer: A

Explanation:
Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.

NEW QUESTION 210
- (Topic 1)
Who should be responsible for network security operations?

A. Business unit managers
B. Security administrators
C. Network administrators
D. IS auditors

Answer: B

Explanation:
Security administrators are usually responsible for network security operations.

NEW QUESTION 213
- (Topic 1)
Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

A. True
B. False

Answer: A

Explanation:
Proper segregation of duties does not prohibit a quality-control administrator from also being responsible for change control and problem management.

NEW QUESTION 214
- (Topic 1)
How is the risk of improper file access affected upon implementing a database system?

A. Risk varie
B. Risk is reduce
C. Risk is not affecte
D. Risk is increase

Answer: D

Explanation:
Improper file access becomes a greater risk when implementing a database system.

NEW QUESTION 218
- (Topic 1)
When reviewing print systems spooling, an IS auditor is MOST concerned with which of the following vulnerabilities?

A. The potential for unauthorized deletion of report copies
B. The potential for unauthorized modification of report copies
C. The potential for unauthorized printing of report copies
D. The potential for unauthorized editing of report copies

Answer: C

Explanation:
When reviewing print systems spooling, an IS auditor is most concerned with the potential for unauthorized printing of report copies.

NEW QUESTION 222
- (Topic 1)
What supports data transmission through split cable facilities or duplicate cable facilities?

A. Diverse routing
B. Dual routing
C. Alternate routing
D. Redundant routing

Answer: A

Explanation:

Diverse routing supports data transmission through split cable facilities, or duplicate cable facilities.

NEW QUESTION 223
- (Topic 1)
What type(s) of firewalls provide(s) the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic?

A. A first-generation packet-filtering firewall
B. A circuit-level gateway
C. An application-layer gateway, or proxy firewall, and stateful-inspection firewalls
D. An application-layer gateway, or proxy firewall, but not stateful-inspection firewalls

Answer: C

Explanation:
An application-layer gateway, or proxy firewall, and stateful-inspection firewalls provide the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic.

NEW QUESTION 228
- (Topic 1)
Which of the following provide(s) near-immediate recoverability for time-sensitive systems and transaction processing?

A. Automated electronic journaling and parallel processing
B. Data mirroring and parallel processing
C. Data mirroring
D. Parallel processing

Answer: B

Explanation:
Data mirroring and parallel processing are both used to provide near-immediate recoverability for time-sensitive systems and transaction processing.

NEW QUESTION 230
- (Topic 1)
What is a common vulnerability, allowing denial-of-service attacks?

A. Assigning access to users according to the principle of least privilege
B. Lack of employee awareness of organizational security policies
C. Improperly configured routers and router access lists
D. Configuring firewall access rules

Answer: C

Explanation:
Improperly configured routers and router access lists are a common vulnerability for denial-of-service attacks.

NEW QUESTION 231
- (Topic 1)
What are trojan horse programs? Choose the BEST answer.

A. A common form of internal attack
B. Malicious programs that require the aid of a carrier program such as email
C. Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
D. A common form of Internet attack

Answer: D

Explanation:
Trojan horse programs are a common form of Internet attack.

NEW QUESTION 234
- (Topic 1)
What is/are used to measure and ensure proper network capacity management and availability of services? Choose the BEST answer.

A. Network performance-monitoring tools
B. Network component redundancy
C. Syslog reporting
D. IT strategic planning

Answer: A

Explanation:
Network performance-monitoring tools are used to measure and ensure proper network capacity management and availability of services.

NEW QUESTION 237
- (Topic 1)
What can be used to gather evidence of network attacks?

A. Access control lists (ACL)
B. Intrusion-detection systems (IDS)
C. Syslog reporting
D. Antivirus programs

Answer: B

Explanation:
Intrusion-detection systems (IDS) are used to gather evidence of network attacks.

NEW QUESTION 242
- (Topic 1)
Which of the following fire-suppression methods is considered to be the most environmentally friendly?

A. Halon gas
B. Deluge sprinklers
C. Dry-pipe sprinklers
D. Wet-pipe sprinklers

Answer: C

Explanation:
Although many methods of fire suppression exist, dry-pipe sprinklers are considered to be the most environmentally friendly.

NEW QUESTION 244
- (Topic 1)
Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key. True or false?

A. False
B. True

Answer: B

Explanation:
Digital signatures require the sender to "sign" the data by encrypting the data with the sender's private key, to then be decrypted by the recipient using the sender's public key.

NEW QUESTION 246
- (Topic 1)
Which of the following provides the BEST single-factor authentication?

A. Biometrics
B. Password
C. Token
D. PIN

Answer: A

Explanation:
Although biometrics provides only single-factor authentication, many consider it to be an excellent method for user authentication.

NEW QUESTION 249
- (Topic 1)
What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

A. An organizational certificate
B. A user certificate
C. A website certificate
D. Authenticode

Answer: C

Explanation:
A website certificate is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption.

NEW QUESTION 254
- (Topic 1)
What determines the strength of a secret key within a symmetric key cryptosystem?

A. A combination of key length, degree of permutation, and the complexity of the data-encryption algorithm that uses the key
B. A combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key
C. A combination of key length and the complexity of the data-encryption algorithm that uses the key
D. Initial input vectors and the complexity of the data-encryption algorithm that uses the key

Answer: B

Explanation:
The strength of a secret key within a symmetric key cryptosystem is determined by a combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key.

NEW QUESTION 258
- (Topic 1)
What process is used to validate a subject's identity?

A. Identification
B. Nonrepudiation
C. Authorization
D. Authentication

Answer: D

Explanation:
Authentication is used to validate a subject's identity.

NEW QUESTION 263
- (Topic 1)
What is often assured through table link verification and reference checks?

A. Database integrity
B. Database synchronization
C. Database normalcy
D. Database accuracy

Answer: A

Explanation:
Database integrity is most often ensured through table link verification and reference checks.

NEW QUESTION 267
- (Topic 1)
What should IS auditors always check when auditing password files?

A. That deleting password files is protected
B. That password files are encrypted
C. That password files are not accessible over the network
D. That password files are archived

Answer: B

Explanation:
IS auditors should always check to ensure that password files are encrypted.

NEW QUESTION 268
- (Topic 1)
Using the OSI reference model, what layer(s) is/are used to encrypt data?

A. Transport layer
B. Session layer
C. Session and transport layers
D. Data link layer

Answer: C

Explanation:
User applications often encrypt and encapsulate data using protocols within the OSI session layer or farther down in the transport layer.

NEW QUESTION 271
- (Topic 1)
When should systems administrators first assess the impact of applications or systems patches?

A. Within five business days following installation
B. Prior to installation
C. No sooner than five business days following installation
D. Immediately following installation

Answer: B

Explanation:
Systems administrators should always assess the impact of patches before installation.

NEW QUESTION 274
- (Topic 1)

Which of the following is the most fundamental step in preventing virus attacks?

A. Adopting and communicating a comprehensive antivirus policy
B. Implementing antivirus protection software on users' desktop computers
C. Implementing antivirus content checking at all network-to-Internet gateways
D. Inoculating systems with antivirus code

Answer: A

Explanation:
 Adopting and communicating a comprehensive antivirus policy is the most fundamental step in preventing virus attacks. All other antivirus prevention efforts rely upon decisions established and communicated via policy.

NEW QUESTION 275
- (Topic 1)
What are intrusion-detection systems (IDS) primarily used for?

A. To identify AND prevent intrusion attempts to a network
B. To prevent intrusion attempts to a network
C. Forensic incident response
D. To identify intrusion attempts to a network

Answer: D

Explanation:
 Intrusion-detection systems (IDS) are used to identify intrusion attempts on a network.

NEW QUESTION 280
- (Topic 1)
If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions. True or false?

A. True
B. False

Answer: A

Explanation:
 If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions.

NEW QUESTION 284
- (Topic 1)
If a database is restored from information backed up before the last system image, which of the following is recommended?

A. The system should be restarted after the last transactio
B. The system should be restarted before the last transactio
C. The system should be restarted at the first transactio
D. The system should be restarted on the last transactio

Answer: B

Explanation:
 If a database is restored from information backed up before the last system image, the system should be restarted before the last transaction because the final transaction must be reprocessed.

NEW QUESTION 287
- (Topic 1)
An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

A. True
B. False

Answer: B

Explanation:
 An off-site processing facility should not be easily identifiable externally because easy identification would create an additional vulnerability for sabotage.

NEW QUESTION 289
- (Topic 1)
Mitigating the risk and impact of a disaster or business interruption usually takes priority over transference of risk to a third party such as an insurer. True or false?

A. True
B. False

Answer: A

Explanation:
Mitigating the risk and impact of a disaster or business interruption usually takes priority over transferring risk to a third party such as an insurer.

NEW QUESTION 294
- (Topic 1)
Off-site data storage should be kept synchronized when preparing for recovery of time-sensitive data such as that resulting from which of the following? Choose the BEST answer.

A. Financial reporting
B. Sales reporting
C. Inventory reporting
D. Transaction processing

Answer: D

Explanation:
Off-site data storage should be kept synchronized when preparing for the recovery of timesensitive data such as that resulting from transaction processing.

NEW QUESTION 295
- (Topic 1)
Why is a clause for requiring source code escrow in an application vendor agreement important?

A. To segregate systems development and live environments
B. To protect the organization from copyright disputes
C. To ensure that sufficient code is available when needed
D. To ensure that the source code remains available even if the application vendor goes out of business

Answer: D

Explanation:
A clause for requiring source code escrow in an application vendor agreement is important to ensure that the source code remains available even if the application vendor goes out of business.

NEW QUESTION 299
- (Topic 1)
What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

A. Assigning copyright to the organization
B. Program back doors
C. Source code escrow
D. Internal programming expertise

Answer: C

Explanation:
Source code escrow protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business.

NEW QUESTION 303
- (Topic 1)
Who is ultimately responsible for providing requirement specifications to the software-development team?

A. The project sponsor
B. The project members
C. The project leader
D. The project steering committee

Answer: A

Explanation:
The project sponsor is ultimately responsible for providing requirement specifications to the software-development team.

NEW QUESTION 306
- (Topic 1)
What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?

A. Contrived data
B. Independently created data
C. Live data
D. Data from previous tests

Answer: D

Explanation:
Regression testing should use data from previous tests to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors.

NEW QUESTION 309
- (Topic 1)
What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality? Choose the BEST answer.

A. Rapid application development (RAD)
B. GANTT
C. PERT
D. Decision trees

Answer: A

Explanation:
Rapid application development (RAD) is used to develop strategically important systems faster, reduce development costs, and still maintain high quality.

NEW QUESTION 311
- (Topic 1)
Test and development environments should be separated. True or false?

A. True
B. False

Answer: A

Explanation:
Test and development environments should be separated, to control the stability of the test environment.

NEW QUESTION 313
- (Topic 1)
Which of the following uses a prototype that can be updated continually to meet changing user or business requirements?

A. PERT
B. Rapid application development (RAD)
C. Function point analysis (FPA)
D. GANTT

Answer: B

Explanation:
Rapid application development (RAD) uses a prototype that can be updated continually to meet changing user or business requirements.

NEW QUESTION 314
- (Topic 1)
What is the most common reason for information systems to fail to meet the needs of users? Choose the BEST answer.

A. Lack of funding
B. Inadequate user participation during system requirements definition
C. Inadequate senior management participation during system requirements definition
D. Poor IT strategic planning

Answer: B

Explanation:
Inadequate user participation during system requirements definition is the most common reason for information systems to fail to meet the needs of users.

NEW QUESTION 315
- (Topic 1)
Input/output controls should be implemented for which applications in an integrated systems environment?

A. The receiving application
B. The sending application
C. Both the sending and receiving applications
D. Output on the sending application and input on the receiving application

Answer: C

Explanation:
Input/output controls should be implemented for both the sending and receiving applications in an integrated systems environment

NEW QUESTION 318
- (Topic 1)
Authentication techniques for sending and receiving data between EDI systems is crucial to prevent which of the following? Choose the BEST answer.

A. Unsynchronized transactions
B. Unauthorized transactions
C. Inaccurate transactions
D. Incomplete transactions

Answer: B

Explanation:
Authentication techniques for sending and receiving data between EDI systems are crucial to prevent unauthorized transactions.

NEW QUESTION 320
- (Topic 1)
What is the primary security concern for EDI environments? Choose the BEST answer.

A. Transaction authentication
B. Transaction completeness
C. Transaction accuracy
D. Transaction authorization

Answer: D

Explanation:
Transaction authorization is the primary security concern for EDI environments.

NEW QUESTION 323
- (Topic 1)
When should an application-level edit check to verify that availability of funds was completed at the electronic funds transfer (EFT) interface?

A. Before transaction completion
B. Immediately after an EFT is initiated
C. During run-to-run total testing
D. Before an EFT is initiated

Answer: D

Explanation:
An application-level edit check to verify availability of funds should be completed at the electronic funds transfer (EFT) interface before an EFT is initiated.

NEW QUESTION 324
- (Topic 1)
Data edits are implemented before processing and are considered which of the following? Choose the BEST answer.

A. Deterrent integrity controls
B. Detective integrity controls
C. Corrective integrity controls
D. Preventative integrity controls

Answer: D

Explanation:
Data edits are implemented before processing and are considered preventive integrity controls.

NEW QUESTION 327
- (Topic 1)
Processing controls ensure that data is accurate and complete, and is processed only through which of the following? Choose the BEST answer.

A. Documented routines
B. Authorized routines
C. Accepted routines
D. Approved routines

Answer: B

Explanation:
Processing controls ensure that data is accurate and complete, and is processed only through authorized routines.

NEW QUESTION 331
- (Topic 1)
An IS auditor is using a statistical sample to inventory the tape library. What type of test would this be considered?

A. Substantive
B. Compliance
C. Integrated
D. Continuous audit

Answer: A

Explanation:
Using a statistical sample to inventory the tape library is an example of a substantive test.

NEW QUESTION 332

- (Topic 2)
An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

A. variable samplin
B. substantive testin
C. compliance testin
D. stop-or-go samplin

Answer: C

Explanation:

Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing, such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

NEW QUESTION 336
- (Topic 2)
Overall business risk for a particular threat can be expressed as:

A. a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerabilit
B. the magnitude of the impact should a threat source successfully exploit the vulnerabilit
C. the likelihood of a given threat source exploiting a given vulnerabilit
D. the collective judgment of the risk assessment tea

Answer: A

Explanation:

Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset. Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process.

NEW QUESTION 340
- (Topic 2)
Which of the following is a substantive test?

A. Checking a list of exception reports
B. Ensuring approval for parameter changes
C. Using a statistical sample to inventory the tape library
D. Reviewing password history reports

Answer: C

Explanation:

A substantive test confirms the integrity of actual processing. A substantive test would determine if the tape library records are stated correctly. A compliance test determines if controls are being applied in a manner that is consistent with management policies and procedures. Checking the authorization of exception reports, reviewing authorization for changing parameters and reviewing password history reports are all compliance tests.

NEW QUESTION 342
- (Topic 2)
An audit charter should:

A. be dynamic and change often to coincide with the changing nature of technology and the audit professio
B. clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal control
C. document the audit procedures designed to achieve the planned audit objective
D. outline the overall authority, scope and responsibilities of the audit functio

Answer: D

Explanation:

An audit charter should state management's objectives for and delegation of authority to IS audit. This charter should not significantly change over time and should be approved at the highest level of management. An audit charter would not be at a detailed level and, therefore, would not include specific audit objectives or procedures.

NEW QUESTION 345
- (Topic 2)
The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

A. information assets are overprotecte
B. a basic level of protection is applied regardless of asset valu
C. appropriate levels of protection are applied to information asset
D. an equal proportion of resources are devoted to protecting all information asset

Answer: C

Explanation:

Full risk assessment determines the level of protection most appropriate to a given level of risk, while the baseline approach merely applies a standard set of protection regardless of risk. There is a cost advantage in not overprotecting information. However, an even bigger advantage is making sure that no information assets are over- or underprotected. The risk assessment approach will ensure an appropriate level of protection is applied, commensurate with the level of risk and asset value and, therefore, considering asset value. The baseline approach does not allow more resources to be directed toward the assets at greater risk, rather than equally directing resources to all assets.

NEW QUESTION 349
- (Topic 2)
Which of the following sampling methods is MOST useful when testing for compliance?

A. Attribute sampling
B. Variable sampling
C. Stratified mean per unit
D. Difference estimation

Answer: A

Explanation:

Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testingto confirm whether the quality exists. The other choices are used in substantive testing, which involves testing of details or quantity.

NEW QUESTION 354
- (Topic 2)
To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

A. schedule the audits and monitor the time spent on each audi
B. train the IS audit staff on current technology used in the compan
C. develop the audit plan on the basis of a detailed risk assessmen
D. monitor progress of audits and initiate cost control measure

Answer: C

Explanation:

Monitoring the time (choice A) and audit programs {choice D), as well as adequate training (choice B), will improve the IS audit staff's productivity (efficiency and performance), but that which delivers value to the organization are the resources and efforts being dedicated to, and focused on, the higher-risk areas.

NEW QUESTION 356
- (Topic 2)
An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

A. the controls already in plac
B. the effectiveness of the controls in plac
C. the mechanism for monitoring the risks related to the asset
D. the threats/vulnerabilities affecting the asset

Answer: D

Explanation:

One of the key factors to be considered while assessing the risks related to the use of various information systems is the threats and vulnerabilities affecting the assets. The risks related to the use of information assets should be evaluated in isolation from the installed controls. Similarly, the effectiveness of the controls should be considered during the risk mitigation stage and not during the risk assessment phase A mechanism to continuously monitor the risks related to assets should be put in place during the risk monitoring function that follows the risk assessment phase.

NEW QUESTION 359
- (Topic 2)
In planning an audit, the MOST critical step is the identification of the:

A. areas of high ris
B. skill sets of the audit staf
C. test steps in the audi
D. time allotted for the audi

Answer: A

Explanation:

When designing an audit plan, it is important to identify the areas of highest risk to determine the areas to be audited. The skill sets of the audit staff should have been considered before deciding and selecting the audit. Test steps for the auditare not as critical as identifying the areas of risk, and the time allotted for an audit is determined by the areas to be audited, which are primarily selected based on the identification of risks.

NEW QUESTION 362
- (Topic 2)
While planning an audit, an assessment of risk should be made to provide:

A. reasonable assurance that the audit will cover material item
B. definite assurance that material items will be covered during the audit wor
C. reasonable assurance that all items will be covered by the audi
D. sufficient assurance that all items will be covered during the audit wor

Answer: A

Explanation:

The ISACA IS Auditing Guideline G15 on planning the IS audit states, 'An assessment of risk should be made to provide reasonable assurance that material items will be adequately covered during the audit work. This assessment should identify areas with a relatively high risk of the existence of material problems.' Definite assurance that material items will be covered during the audit work is an impractical proposition. Reasonable assurance that all items will be covered during the audit work is not the correct answer, as material items need to be covered, not all items.

NEW QUESTION 366
- (Topic 2)
An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

A. the probability of error must be objectively quantifie
B. the auditor wishes to avoid sampling ris
C. generalized audit software is unavailabl
D. the tolerable error rate cannot be determine

Answer: A

Explanation:

Given an expected error rate and confidence level, statistical sampling is an objective method of sampling, which helps an IS auditor determine the sample size and quantify the probability of error (confidence coefficient). Choice B is incorrect because sampling risk is the risk of a sample not being representative of the population. This risk exists for both judgment and statistical samples. Choice C is incorrect because statistical sampling does not require the use of generalized audit software. Choice D is incorrect because the tolerable error rate must be predetermined for both judgment and statistical sampling.

NEW QUESTION 369
- (Topic 2)
An IS auditor evaluating logical access controls should FIRST:

A. document the controls applied to the potential access paths to the syste
B. test controls over the access paths to determine if they are functiona
C. evaluate the security environment in relation to written policies and practices
D. obtain an understanding of the security risks to information processin

Answer: D

Explanation:

When evaluating logical access controls, an IS auditor should first obtain an understanding of the security risks facing information processing by reviewing relevant documentation, by inquiries, and by conducting a risk assessment. Documentation andevaluation is the second step in assessing the adequacy, efficiency and effectiveness, thus identifying deficiencies or redundancy in controls. The third step is to test the access paths-to determine if the controls are functioning. Lastly, theIS auditor evaluates the security environment to assess its adequacy by reviewing the written policies, observing practices and comparing them to appropriate security best practices.

NEW QUESTION 373
- (Topic 2)
The PRIMARY purpose of an IT forensic audit is:

A. to participate in investigations related to corporate frau
B. the systematic collection of evidence after a system irregularit
C. to assess the correctness of an organization's financial statements
D. to determine that there has been criminal activit

Answer: B

Explanation:

Choice B describes a forensic audit. The evidence collected could then be used in judicial proceedings. Forensic audits are not limited to corporate fraud. Assessing the correctness of an organization's financial statements is not the purpose of a forensic audit. Drawing a conclusion as to criminal activity would be part of a legal process and not the objective of a forensic audit.

NEW QUESTION 378
- (Topic 2)
In an IS audit of several critical servers, the IS auditor wants to analyze audit trails to discover potential anomalies in user or system behavior. Which of the following tools are MOST suitable for performing that task?

A. CASE tools
B. Embedded data collection tools

C. Heuristic scanning tools
D. Trend/variance detection tools

Answer: D

Explanation:

Trend/variance detection tools look for anomalies in user or system behavior, for example, determining whether the numbers for prenumbered documents are sequential or increasing. CASE tools are used to assist software development. Embedded (audit) data collection software is used for sampling and to provide production statistics. Heuristic scanning tools can be used to scan for viruses to indicate possible infected code.

NEW QUESTION 381
- (Topic 2)
An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

A. There are a number of external modems connected to the networ
B. Users can install software on their desktop
C. Network monitoring is very limite
D. Many user IDs have identical password

Answer: D

Explanation:

Exploitation of a known user ID and password requires minimal technical knowledge and exposes the network resources to exploitation. The technical barrier is low and the impact can be very high; therefore, the fact that many user IDs have identical passwords represents the greatest threat. External modems represent a security risk, but exploitation still depends on the use of a valid user account. While the impact of users installing software on their desktops can be high {for example, due to the installation of Trojans or key-logging programs), the likelihood is not high due to the level of technical knowledge required to successfully penetrate the network. Although network monitoring can be a useful detective control, it will only detectabuse of user accounts in special circumstances and is, therefore, not a first line of defense.

NEW QUESTION 383
- (Topic 2)
Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

A. The preservation of the chain of custody for electronic evidence
B. Time and cost savings
C. Efficiency and effectiveness
D. Ability to search for violations of intellectual property rights

Answer: A

Explanation:

The primary objective of forensic software is to preserve electronic evidence to meet the rules of evidence. Choice B, time and cost savings, and choice C, efficiency and effectiveness, are legitimate concerns that differentiate good from poor forensic software packages. Choice D, the ability to search for intellectual property rights violations, is an example of a use of forensic software.

NEW QUESTION 384
- (Topic 2)
An IS auditor has imported data from the client's database. The next step-confirming whether the imported data are complete-is performed by:

A. matching control totals of the imported data to control totals of the original dat
B. sorting the data to confirm whether the data are in the same order as the original dat
C. reviewing the printout of the first 100 records of original data with the first 100 records of imported dat
D. filtering data for different categories and matching them to the original dat

Answer: A

Explanation:

Matching control totals of the imported data with control totals of the original data is the next logical step, as this confirms the completeness of the imported datA. It is not possible to confirm completeness by sorting the imported data, because the original data may not be in sorted order. Further, sorting does not provide control totals for verifying completeness. Reviewing a printout of 100 records of original data with 100 records of imported data is a process of physical verification andconfirms the accuracy of only these records. Filtering data for different categories and matching them to original data would still require that control totals be developed to confirm the completeness of the data.

NEW QUESTION 388
- (Topic 2)
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

A. create the procedures documen
B. terminate the audi
C. conduct compliance testin
D. identify and evaluate existing practice

Answer: D

Explanation:

One of the main objectives of an audit is to identify potential risks; therefore, the most proactive approach would be to identify and evaluate the existing security practices being followed by the organization. IS auditors should not prepare documentation, as doing so could jeopardize their independence. Terminating the audit may prevent achieving one of the basic audit objectives, i.e., identification of potential risks. Since there are no documented procedures, there is no basis against whichto test compliance.

NEW QUESTION 389
- (Topic 2)
Which of the following should be of MOST concern to an IS auditor?

A. Lack of reporting of a successful attack on the network
B. Failure to notify police of an attempted intrusion
C. Lack of periodic examination of access rights
D. Lack of notification to the public of an intrusion

Answer: A

Explanation:

Not reporting an intrusion is equivalent to an IS auditor hiding a malicious intrusion, which would be a professional mistake. Although notification to the police may be required and the lack of a periodic examination of access rights might be a concern, they do not represent as big a concern as the failure to report the attack. Reporting to the public is not a requirement and is dependent on the organization's desire, or lack thereof, to make the intrusion known.

NEW QUESTION 393
- (Topic 2)
Which of the following would normally be the MOST reliable evidence for an auditor?

A. A confirmation letter received from a third party verifying an account balance
B. Assurance from line management that an application is working as designed
C. Trend data obtained from World Wide Web (Internet) sources
D. Ratio analysts developed by the IS auditor from reports supplied by line management

Answer: A

Explanation:

Evidence obtained from independent third parties almost always is considered to be the most reliable. Choices B, C and D would not be considered as reliable.

NEW QUESTION 398
- (Topic 2)
When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

A. The point at which controls are exercised as data flow through the system
B. Only preventive and detective controls are relevant
C. Corrective controls can only be regarded as compensating
D. Classification allows an IS auditor to determine which controls are missing

Answer: A

Explanation:

An IS auditor should focus on when controls are exercised as data flow through a computer system. Choice B is incorrect since corrective controls may also be relevant. Choice C is incorrect, since corrective controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is incorrect and irrelevant since the existence and function of controls is important, not the classification.

NEW QUESTION 400
- (Topic 2)
Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

A. Discussion with management
B. Review of the organization chart
C. Observation and interviews
D. Testing of user access rights

Answer: C

Explanation:

By observing the IS staff performing their tasks, an IS auditor can identify whether they are performing any incompatible operations, and by interviewing the IS staff, the auditor can get an overview of the tasks performed. Based on the observationsand interviews the auditor can evaluate the segregation of duties. Management may not be aware of the detailed functions of each employee in the IS department; therefore, discussion with the management would provide only limited information regardingsegregation of duties. An organization chart would not provide details of the functions of the employees. Testing of user rights would provide information about the rights they have within the IS systems, but would not provide complete information about the functions they perform.

NEW QUESTION 401
- (Topic 2)

During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

A. test data to validate data inpu
B. test data to determine system sort capabilitie
C. generalized audit software to search for address field duplication
D. generalized audit software to search for account field duplication

Answer: C

Explanation:

Since the name is not the same {due to name variations), one method to detect duplications would be to compare other common fields, such as addresses. A subsequent review to determine common customer names at these addresses could then be conducted. Searching for duplicate account numbers would not likely find duplications, since customers would most likely have different account numbers for each variation. Test data would not be useful to detect the extent of any data characteristic, but simply to determine how the data were processed.

NEW QUESTION 406
- (Topic 2)
Which of the following would be the BEST population to take a sample from when testing program changes?

A. Test library listings
B. Source program listings
C. Program change requests
D. Production library listings

Answer: D

Explanation:

The best source from which to draw any sample or test of system information is the automated system. The production libraries represent executables that are approved and authorized to process organizational datA. Source program listings would be timeintensive. Program change requests are the documents used to initiate change; there is no guarantee that the request has been completed for all changes. Test library listings do not represent the approved and authorized executables.

NEW QUESTION 408
- (Topic 2)
Which of the following forms of evidence for the auditor would be considered the MOST reliable?

A. An oral statement from the auditee
B. The results of a test performed by an IS auditor
C. An internally generated computer accounting report
D. A confirmation letter received from an outside source

Answer: D

Explanation:

Evidence obtained from outside sources is usually more reliable than that obtained from within the organization. Confirmation letters received from outside parties, such as those used to verify accounts receivable balances, are usually highly reliable. Testing performed by an auditor may not be reliable, if the auditor did not have a good understanding of the technical area under review.

NEW QUESTION 410
- (Topic 2)
An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

A. Availability of online network documentation
B. Support of terminal access to remote hosts
C. Handling file transfer between hosts and interuser communications
D. Performance management, audit and control

Answer: A

Explanation:

Network operating system user features include online availability of network documentation. Other features would be user access to various resources of network hosts, user authorization to access particular resources, and the network and host computers used without special user actions or commands. Choices B, C and D are examples of network operating systems functions.

NEW QUESTION 415
- (Topic 2)
Which of the following is an advantage of an integrated test facility (ITF)?

A. It uses actual master files or dummies and the IS auditor does not have to review the source of the transactio
B. Periodic testing does not require separate test processe
C. It validates application systems and tests the ongoing operation of the syste
D. The need to prepare test data is eliminate

Answer: B

Explanation:

An integrated test facility creates a fictitious entity in the database to process test transactions simultaneously with live input. Its advantage is that periodic testing does not require separate test processes. However, careful planning is necessary, and test data must be isolated from production data.

NEW QUESTION 417
- (Topic 2)
An IS auditor evaluates the test results of a modification to a system that deals with payment computation. The auditor finds that 50 percent of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?

A. Design further tests of the calculations that are in erro
B. Identify variables that may have caused the test results to be inaccurat
C. Examine some of the test cases to confirm the result
D. Document the results and prepare a report of findings, conclusions and recommendation

Answer: C

Explanation:

An IS auditor should next examine cases where incorrect calculations occurred and confirm the results. After the calculations have been confirmed, further tests can be conducted and reviewed. Report preparation, findings and recommendations would notbe made until all results are confirmed.

NEW QUESTION 421
- (Topic 2)
The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs
B. recreating program logic using generalized audit software to calculate monthly total
C. preparing simulated transactions for processing and comparing the results to predetermined result
D. automatic flowcharting and analysis of the source code of the calculation program

Answer: C

Explanation:

Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

NEW QUESTION 426
- (Topic 2)
Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

A. Embedded audit module
B. Integrated test facility
C. Snapshots
D. Audit hooks

Answer: D

Explanation:

The audit hook technique involves embedding code in application systems for the examination of selected transactions. This helps an IS auditor to act before an error or an irregularity gets out of hand. An embedded audit module involves embedding specially-written software in the organization's host application system so that application systems are monitored on a selective basis. An integrated test facility is used when it is not practical to use test data, and snapshots are used when an audittrail is required.

NEW QUESTION 430
- (Topic 2)
A substantive test to verify that tape library inventory records are accurate is:

A. determining whether bar code readers are installe
B. determining whether the movement of tapes is authorize
C. conducting a physical count of the tape inventor
D. checking if receipts and issues of tapes are accurately recorde

Answer: C

Explanation:

A substantive test includes gathering evidence to evaluate the integrity of individual transactions, data or other information. Conducting a physical count of the tape inventory is a substantive test. Choices A, B and D are compliance tests.

NEW QUESTION 431
- (Topic 2)
An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

A. conclude that the controls are inadequat
B. expand the scope to include substantive testin
C. place greater reliance on previous audit
D. suspend the audi

Answer: B

Explanation:

If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of testing the controls and include additional substantive tests. There is no evidence that whatever controls might exist are either inadequate or adequate. Placing greater reliance on previous audits or suspending the audit are inappropriate actions as they provide no current knowledge of the adequacy of the existing controls.

NEW QUESTION 436
- (Topic 2)
An IS auditor issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommends a vendor product to address this vulnerability. The IS auditor has failed to exercise:

A. professional independence
B. organizational independenc
C. technical competenc
D. professional competenc

Answer: A

Explanation:

When an IS auditor recommends a specific vendor, they compromise professional independence. Organizational independence has no relevance to the content of an audit report and should be considered at the time of accepting the engagement. Technical and professional competence is not relevant to the requirement of independence.

NEW QUESTION 440
- (Topic 2)
The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

A. understand the business proces
B. comply with auditing standard
C. identify control weaknes
D. plan substantive testin

Answer: A

Explanation:

Understanding the business process is the first step an IS auditor needs to perform. Standards do not require an IS auditor to perform a process walkthrough. Identifying control weaknesses is not the primary reason for the walkthrough and typically occurs at a later stage in the audit, while planning for substantive testing is performed at a later stage in the audit.

NEW QUESTION 442
- (Topic 2)
In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

A. examine source program changes without information from IS personne
B. detect a source program change made between acquiring a copy of the source and the comparison ru
C. confirm that the control copy is the current version of the production progra
D. ensure that all changes made in the current source copy are detecte

Answer: A

Explanation:

An IS auditor has an objective, independent and relatively complete assurance of program changes because the source code comparison will identify changes. Choice B is incorrect, because the changes made since the acquisition of the copy are not included in the copy of the software. Choice C is incorrect, as an IS auditor will have to gain this assurance separately. Choice D is incorrect, because any changes made between the time the control copy was acquired and the source code comparison is made will not be detected.

NEW QUESTION 446
- (Topic 2)
Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

A. include the statement of management in the audit repor
B. identify whether such software is, indeed, being used by the organizatio
C. reconfirm with management the usage of the softwar
D. discuss the issue with senior management since reporting this could have a negative impact on the organizatio

Answer: B

Explanation:

When there is an indication that an organization might be using unlicensed software, the IS auditor should obtain sufficient evidence before including it in the report. With respect to this matter, representations obtained from management cannot be independently verified. If the organization is using software that is not licensed, the auditor, to maintain objectivity and independence, must include this in the report.

NEW QUESTION 450
- (Topic 2)
After initial investigation, an IS auditor has reasons to believe that fraud may be present. The IS auditor should:

A. expand activities to determine whether an investigation is warrante
B. report the matter to the audit committe
C. report the possibility of fraud to top management and ask how they would like to procee
D. consult with external legal counsel to determine the course of action to be take

Answer: A

Explanation:

An IS auditor's responsibilities for detecting fraud include evaluating fraud indicators and deciding whether any additional action is necessary or whether an investigation should be recommended. The IS auditor should notify the appropriate authorities within the organization only if it has determined that the indicators of fraud are sufficient to recommend an investigation. Normally, the IS auditor does not have authority to consult with external legal counsel.

NEW QUESTION 453
- (Topic 2)
During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

A. Dumping the memory content to a file
B. Generating disk images of the compromised system
C. Rebooting the system
D. Removing the system from the network

Answer: C

Explanation:

Rebooting the system may result in a change in the system state and the loss of files and important evidence stored in memory. The other choices are appropriate actions for preserving evidence.

NEW QUESTION 456
- (Topic 2)
An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

A. Personally delete all copies of the unauthorized softwar
B. Inform the auditee of the unauthorized software, and follow up to confirm deletio
C. Report the use of the unauthorized software and the need to prevent recurrence to auditee managemen
D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such us

Answer: C

Explanation:

The use of unauthorized or illegal software should be prohibited by an organization. Software piracy results in inherent exposure and can result in severe fines. An IS auditor must convince the user and user management of the risk and the need to eliminate the risk. An IS auditor should not assume the role of the enforcing officer and take on any personal involvement in removing or deleting the unauthorized software.

NEW QUESTION 458
- (Topic 2)
During an implementation review of a multiuser distributed application, an IS auditor finds minor weaknesses in three areas-the initial setting of parameters is improperly installed, weak passwords are being used and some vital reports are not beingchecked properly. While preparing the audit report, the IS auditor should:

A. record the observations separately with the impact of each of them marked against each respective findin
B. advise the manager of probable risks without recording the observations, as the control weaknesses are minor one
C. record the observations and the risk arising from the collective weaknesse
D. apprise the departmental heads concerned with each observation and properly document it in the repor

Answer: C

Explanation:

Individually the weaknesses are minor; however, together they have the potential to substantially weaken the overall control structure. Choices A and D reflect a failure on the part of an IS auditor to recognize the combined affect of the control weakness. Advising the local manager without reporting the facts and observations would conceal the findings from other stakeholders.

NEW QUESTION 459

- (Topic 2)
A PRIMARY benefit derived from an organization employing control self-assessment (CSA) techniques is that it:

A. can identify high-risk areas that might need a detailed review late
B. allows IS auditors to independently assess ris
C. can be used as a replacement for traditional audit
D. allows management to relinquish responsibility for contro

Answer: A

Explanation:

CSA is predicated on the review of high-risk areas that either need immediate attention or a more thorough review at a later date. Choice B is incorrect, because CSA requires the involvement of auditors and line management. What occurs is that the internal audit function shifts some of the control monitoring responsibilities to the functional areas. Choice C is incorrect because CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them. Choice D is incorrect, because CSA does not allow management to relinquish its responsibility for control.

NEW QUESTION 463
- (Topic 2)
Which of the following is the key benefit of control self-assessment (CSA)?

A. Management ownership of the internal controls supporting business objectives is reinforce
B. Audit expenses are reduced when the assessment results are an input to external audit wor
C. Improved fraud detection since internal business staff are engaged in testing controls
D. Internal auditors can shift to a consultative approach by using the results of the assessmen

Answer: A

Explanation:

The objective of control self-assessment is to have business management become more aware of the importance of internal control and their responsibility in terms of corporate governance. Reducing audit expenses is not a key benefit of control self-assessment (CSA). improved fraud detection is important, but not as important as ownership, and is not a principal objective of CSA. CSA may give more insights to internal auditors, allowing them to take a more consultative role; however, this is an additional benefit, not the key benefit.

NEW QUESTION 467
- (Topic 3)
An IT steering committee should review information systems PRIMARILY to assess:

A. whether IT processes support business requirement
B. if proposed system functionality is adequat
C. the stability of existing softwar
D. the complexity of installed technolog

Answer: A

Explanation:

The role of an IT steering committee is to ensure that the IS department is in harmony with the organization's mission and objectives. To ensure this, the committee must determine whether IS processes support the business requirements. Assessing proposed additional functionality and evaluating software stability and the complexity of technology are too narrow in scope to ensure that IT processes are, in fact, supporting the organization's goals.

NEW QUESTION 471
- (Topic 3)
The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

A. a lack of investment in technolog
B. a lack of a methodology for systems developmen
C. technology not aligning with the organization's objective
D. an absence of control over technology contract

Answer: C

Explanation:

A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

NEW QUESTION 473
- (Topic 3)
Which of the following is a function of an IS steering committee?

A. Monitoring vendor-controlled change control and testing
B. Ensuring a separation of duties within the information's processing environment
C. Approving and monitoring major projects, the status of IS plans and budgets
D. Liaising between the IS department and the end users

Answer: C

Explanation:

The IS steering committee typically serves as a general review board for major IS projects and should not become involved in routine operations; therefore, one of its functions is to approve and monitor major projects, the status of IS plans and budgets. Vendor change control is an outsourcing issue and should be monitored by IS management. Ensuring a separation of duties within the information's processing environment is an IS management responsibility. Liaising between the IS department and the end users is a function of the individual parties and not a committee.

NEW QUESTION 475
- (Topic 3)
Effective IT governance will ensure that the IT plan is consistent with the organization's:

A. business pla
B. audit pla
C. security pla
D. investment pla

Answer: A

Explanation:

To govern IT effectively, IT and business should be moving in the same direction, requiring that the IT plans are aligned with an organization's business plans. The audit and investment plans are not part of the IT plan, while the security plan should be at a corporate level.

NEW QUESTION 480
- (Topic 3)
The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

A. IT budge
B. existing IT environmen
C. business pla
D. investment pla

Answer: C

Explanation:

One of the most important reasons for which projects get funded is how well a project meets an organization's strategic objectives. Portfolio management takes a holistic view of a company's overall IT strategy. IT strategy should be aligned with thebusiness strategy and, hence, reviewing the business plan should be the major consideration. Choices A, B and D are important but secondary to the importance of reviewing the business plan.

NEW QUESTION 484
- (Topic 3)
The ultimate purpose of IT governance is to:

A. encourage optimal use of I
B. reduce IT cost
C. decentralize IT resources across the organizatio
D. centralize control of I

Answer: A

Explanation:

IT governance is intended to specify the combination of decision rights and accountability that is best for the enterprise. It is different for every enterprise. Reducing IT costs may not be the best IT governance outcome for an enterprise. Decentralizing IT resources across the organization is not always desired, although it may be desired in a decentralized environment. Centralizing control of IT is not always desired. An example of where it might be desired is an enterprise desiring a single point of customer contact.

NEW QUESTION 489
- (Topic 3)
Responsibility for the governance of IT should rest with the:

A. IT strategy committe
B. chief information officer (CIO).
C. audit committe
D. board of director

Answer: D

Explanation:

Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. The audit committee, the chief information officer (CIO) and the IT strategy committee all play a significant role in the successful implementation of IT governance within an organization, but the ultimate accountability resides with the board of directors.

NEW QUESTION 491

- (Topic 3)
Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. ensure the employee maintains a good quality of life, which will lead to greater productivit
B. reduce the opportunity for an employee to commit an improper or illegal ac
C. provide proper cross-training for another employe
D. eliminate the potential disruption caused when an employee takes vacation one day at a tim

Answer: B

Explanation:

Required vacations/holidays of a week or more in duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions, as this reduces the opportunity to commit improper or illegal acts. During this time it may be possible to discover any fraudulent activity that was taking place. Choices A, C and D could all be organizational benefits from a mandatory vacation policy, but they are not the reason why the policy is established.

NEW QUESTION 493
- (Topic 3)
A local area network (LAN) administrator normally would be restricted from:

A. having end-user responsibilitie
B. reporting to the end-user manage
C. having programming responsibilitie
D. being responsible for LAN security administratio

Answer: C

Explanation:

A LAN administrator should not have programming responsibilities but may have end-user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator may also be responsible for security administration over the LAN.

NEW QUESTION 496
- (Topic 3)
Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?

A. Senior management is aware of critical information assets and demonstrates an adequate concern for their protectio
B. Job descriptions contain clear statements of accountability for information securit
C. In accordance with the degree of risk and business impact, there is adequate funding for security effort
D. No actual incidents have occurred that have caused a loss or a public embarrassmen

Answer: B

Explanation:

Inclusion in job descriptions of security responsibilities is a form of security training and helps ensure that staff and management are aware of their roles with respect to information security. The other three choices are not criterion for evaluating security awareness training. Awareness is a criterion for evaluating the importance that senior management attaches to information assets and their protection. Funding is a criterion that aids in evaluating whether security vulnerabilities are being addressed, while the number of incidents that have occurred is a criterion for evaluating the adequacy of the risk management program.

NEW QUESTION 499
- (Topic 3)
Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

A. has been approved by line managemen
B. does not vary from the IS department's preliminary budge
C. complies with procurement procedure
D. supports the business objectives of the organizatio

Answer: D

Explanation:

Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals. Choice A is incorrectsince line management prepared the plans.

NEW QUESTION 502
- (Topic 3)
In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

A. Optimized
B. Managed
C. Defined
D. Repeatable

Answer: B

Explanation:

Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable.'

NEW QUESTION 505
- (Topic 3)
When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

A. incorporates state of the art technolog
B. addresses the required operational control
C. articulates the IT mission and visio
D. specifies project management practice

Answer: C

Explanation:

The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls or project management practices.

NEW QUESTION 506
- (Topic 3)
When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

A. establishment of a review boar
B. creation of a security uni
C. effective support of an executive sponso
D. selection of a security process owne

Answer: C

Explanation:

The executive sponsor would be in charge of supporting the organization's strategic security program, and would aid in directing the organization's overall security management activities. Therefore, support by the executive level of management is themost critical success factor (CSF). None of the other choices are effective without visible sponsorship of top management.

NEW QUESTION 508
- (Topic 3)
When reviewing an organization's strategic IT plan an IS auditor should expect to find:

A. an assessment of the fit of the organization's application portfolio with business objective
B. actions to reduce hardware procurement cos
C. a listing of approved suppliers of IT contract resource
D. a description of the technical architecture for the organization's network perimeter securit

Answer: A

Explanation:

An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions. Further assessment can then be made of how well the overall IT organization, encompassing applications, infrastructure, services, management processes, etc., can support the business objectives. Operational efficiency initiatives belong to tactical planning, not strategic planning. The purpose of an IT strategic plan is toset out how IT will be used to achieve or support an organization's business objectives. A listing of approved suppliers of IT contract resources is a tactical rather than a strategic concern. An IT strategic plan would not normally include detail ofa specific technical architecture.

NEW QUESTION 509
- (Topic 3)
The advantage of a bottom-up approach to the development of organizational policies is that the policies:

A. are developed for the organization as a whol
B. are more likely to be derived as a result of a risk assessmen
C. will not conflict with overall corporate polic
D. ensure consistency across the organizatio

Answer: B

Explanation:

A bottom-up approach begins by defining operational-level requirements and policies, which are derived and implemented as the result of risk assessments. Enterprise-level policies are subsequently developed based on a synthesis of existing operational policies. Choices A, C and D are advantages of a top-down approach for developing organizational policies. This approach ensures that the policies will not be in conflict with overall corporate policy and ensure consistency across the organization.

NEW QUESTION 514

- (Topic 3)
An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

A. this lack of knowledge may lead to unintentional disclosure of sensitive informatio
B. information security is not critical to all function
C. IS audit should provide security training to the employee
D. the audit finding will cause management to provide continuous training to staf

Answer: A

Explanation:

All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

NEW QUESTION 519
- (Topic 3)
Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

A. Assimilation of the framework and intent of a written security policy by all appropriate parties
B. Management support and approval for the implementation and maintenance of a security policy
C. Enforcement of security rules by providing punitive actions for any violation of security rules
D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Answer: A

Explanation:

Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules, is also required, along with the user's education on the importance of security.

NEW QUESTION 522
- (Topic 3)
A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

A. recover
B. retentio
C. rebuildin
D. reus

Answer: B

Explanation:

Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the officialform of classic 'paper* makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

NEW QUESTION 524
- (Topic 3)
In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

A. implementatio
B. complianc
C. documentatio
D. sufficienc

Answer: D

Explanation:

An IS auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of controls. Documentation, implementation and compliance are further steps.

NEW QUESTION 529
- (Topic 3)
A top-down approach to the development of operational policies will help ensure:

A. that they are consistent across the organizatio
B. that they are implemented as a part of risk assessmen
C. compliance with all policie
D. that they are reviewed periodicall

Answer: A

Explanation:

Deriving lower level policies from corporate policies {a top-down approach) aids in ensuring consistency across the organization and consistency with other policies. The bottom-up approach to the development of operational policies is derived as a result of risk assessment. A top-down approach of itself does not ensure compliance and development does not ensure that policies are reviewed.

NEW QUESTION 533
- (Topic 3)
Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

A. Time zone differences could impede communications between IT team
B. Telecommunications cost could be much higher in the first yea
C. Privacy laws could prevent cross-border flow of informatio
D. Software development may require more detailed specification

Answer: C

Explanation:

Privacy laws prohibiting the cross-border flow of personally identifiable information would make it impossible to locate a data warehouse containing customer information in another country. Time zone differences and higher telecommunications costs are more manageable. Software development typically requires more detailed specifications when dealing with offshore operations.

NEW QUESTION 535
- (Topic 3)
A retail outlet has introduced radio frequency identification (RFID) tags to create unique serial numbers for all products. Which of the following is the PRIMARY concern associated with this initiative?

A. Issues of privacy
B. Wavelength can be absorbed by the human body
C. RFID tags may not be removable
D. RFID eliminates line-of-sight reading

Answer: A

Explanation:

The purchaser of an item will not necessarily be aware of the presence of the tag. If a tagged item is paid for by credit card, it would be possible to tie the unique ID of that item to the identity of the purchaser. Privacy violations are a significant concern because RFID can carry unique identifier numbers. If desired it would be possible for a firm to track individuals who purchase an item containing an RFID. Choices B and C are concerns of less importance. Choice D is not a concern.

NEW QUESTION 536
- (Topic 3)
When developing a security architecture, which of the following steps should be executed FIRST?

A. Developing security procedures
B. Defining a security policy
C. Specifying an access control methodology
D. Defining roles and responsibilities

Answer: B

Explanation:

Defining a security policy for information and related technology is the first step toward building a security architecture. A security policy communicates a coherent security standard to users, management and technical staff. Security policies willoften set the stage in terms of what tools and procedures are needed for an organization. The other choices should be executed only after defining a security policy.

NEW QUESTION 538
- (Topic 3)
An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should FIRST verify that the:

A. technical platforms between the two companies are interoperabl
B. parent bank is authorized to serve as a service provide
C. security features are in place to segregate subsidiary trade
D. subsidiary can join as a co-owner of this payment syste

Answer: B

Explanation:

Even between parent and subsidiary companies, contractual agreement(s) should be in place to conduct shared services. This is particularly important in highly regulated organizations such as banking. Unless granted to serve as a service provider, itmay not be legal for the bank to extend business to the subsidiary companies. Technical aspects should always be considered; however, this can be initiated after confirming that the parent bank can serve as a service provider. Security aspects are another important factor; however, this should be considered after confirming that the parent bank can serve as a service provider. The ownership of the payment system is not as important as the legal authorization to operate the system.

NEW QUESTION 541

......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your CISA Exam with Our Prep Materials Via below:

https://www.certleader.com/CISA-dumps.html