

Exam Questions CISA

Isaca CISA

<https://www.2passeasy.com/dumps/CISA/>



NEW QUESTION 1

- (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 2

- (Topic 1)

Which of the following is a benefit of using callback devices?

- A. Provide an audit trail
- B. Can be used in a switchboard environment
- C. Permit unlimited user mobility
- D. Allow call forwarding

Answer: A

Explanation:

A callback feature hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches. Call forwarding (choice D) is a means of potentially bypassing callback control. By dialing through an authorized phone number from an unauthorized phone number, a perpetrator can gain computer access. This vulnerability can be controlled through callback systems that are available.

NEW QUESTION 3

- (Topic 1)

Structured programming is BEST described as a technique that:

- A. provides knowledge of program functions to other programmers via peer review
- B. reduces the maintenance time of programs by the use of small-scale program module
- C. makes the readable coding reflect as closely as possible the dynamic execution of the progra
- D. controls the coding and testing of the high-level functions of the program in the development proces

Answer: B

Explanation:

A characteristic of structured programming is smaller, workable units. Structured programming has evolved because smaller, workable units are easier to maintain. Structured programming is a style of programming which restricts the kinds of control structures. This limitation is not crippling. Any program can be written with allowed control structures. Structured programming is sometimes referred to as go-to-less programming, since a go-to statement is not allowed. This is perhaps the most well known restriction of the style, since go-to statements were common at the time structured programming was becoming more popular. Statement labels also become unnecessary, except in languages where subroutines are identified by labels.

NEW QUESTION 4

- (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 5

- (Topic 1)

In an EDI process, the device which transmits and receives electronic documents is the:

- A. communications handle
- B. EDI translato
- C. application interfac
- D. EDI interfac

Answer:

A

Explanation:

A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs).

NEW QUESTION 6

- (Topic 1)

A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

- A. digest signatur
- B. electronic signatur
- C. digital signatur
- D. hash signatur

Answer: C

Explanation:

A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. It is a string of bits that uniquely represent another string of bits, a digital document. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad, connected to the system.

NEW QUESTION 7

- (Topic 1)

Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

- A. Spool
- B. Cluster controller
- C. Protocol converter
- D. Front end processor

Answer: D

Explanation:

A front-end processor is a hardware device that connects all communication lines to a central computer to relieve the central computer.

NEW QUESTION 8

- (Topic 1)

Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?

- A. Multiplexer
- B. Modem
- C. Protocol converter
- D. Concentrator

Answer: B

Explanation:

A modem is a device that translates data from digital to analog and back to digital.

NEW QUESTION 9

- (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 10

- (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 10

- (Topic 1)

Company.com has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

- A. Acceptance testing is to be managed by user
- B. A quality plan is not part of the contracted deliverable
- C. Not all business functions will be available on initial implementation
- D. Prototyping is being used to confirm that the system meets business requirement

Answer: B

Explanation:

A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the proposed development contract should be comprehensive and encompass all phases of the development and include which business functions will be included and when. Acceptance is normally managed by the user area, since they must be satisfied that the new system will meet their requirements. If the system is large, a phased-in approach to implementing the application is a reasonable approach. Prototyping is a valid method of ensuring that the system will meet business requirements.

NEW QUESTION 13

- (Topic 1)

In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

- A. registration authority (RA).
- B. issuing certification authority (CA).
- C. subject C
- D. policy management authority

Answer: A

Explanation:

A RA is an entity that is responsible for identification and authentication of certificate subjects, but the RA does not sign or issue certificates. The certificate subject usually interacts with the RA for completing the process of subscribing to the services of the certification authority in terms of getting identity validated with standard identification documents, as detailed in the certificate policies of the CA. In the context of a particular certificate, the issuing CA is the CA that issued the certificate. In the context of a particular CA certificate, the subject CA is the CA whose public key is certified in the certificate.

NEW QUESTION 14

- (Topic 1)

A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

- A. reasonableness check
- B. parity check
- C. redundancy check
- D. check digit

Answer: C

Explanation:

A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of data.

NEW QUESTION 19

- (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 23

- (Topic 1)

How does the process of systems auditing benefit from using a risk-based approach to audit planning?

- A. Controls testing starts earlier
- B. Auditing resources are allocated to the areas of highest concern
- C. Auditing risk is reduced
- D. Controls testing is more thorough

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 27

- (Topic 1)

After an IS auditor has identified threats and potential impacts, the auditor should:

- A. Identify and evaluate the existing controls
- B. Conduct a business impact analysis (BIA)
- C. Report on existing controls
- D. Propose new controls

Answer: A

Explanation:

After an IS auditor has identified threats and potential impacts, the auditor should then identify and evaluate the existing controls.

NEW QUESTION 28

- (Topic 1)

What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

- A. Business risk
- B. Detection risk
- C. Residual risk
- D. Inherent risk

Answer: B

Explanation:

Detection risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist.

NEW QUESTION 32

- (Topic 1)

A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:

- A. Identify high-risk areas that might need a detailed review later
- B. Reduce audit costs
- C. Reduce audit time
- D. Increase audit accuracy

Answer: C

Explanation:

A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can identify high-risk areas that might need a detailed review later.

NEW QUESTION 36

- (Topic 1)

What type of approach to the development of organizational policies is often driven by risk assessment?

- A. Bottom-up
- B. Top-down
- C. Comprehensive
- D. Integrated

Answer: B

Explanation:

A bottom-up approach to the development of organizational policies is often driven by risk assessment.

NEW QUESTION 41

- (Topic 1)

A core tenant of an IS strategy is that it must:

- A. Be inexpensive
- B. Be protected as sensitive confidential information

- C. Protect information confidentiality, integrity, and availability
- D. Support the business objectives of the organization

Answer: D

Explanation:

Above all else, an IS strategy must support the business objectives of the organization.

NEW QUESTION 44

- (Topic 1)

Which of the following could lead to an unintentional loss of confidentiality? Choose the BEST answer.

- A. Lack of employee awareness of a company's information security policy
- B. Failure to comply with a company's information security policy
- C. A momentary lapse of reason
- D. Lack of security policy enforcement procedures

Answer: A

Explanation:

Lack of employee awareness of a company's information security policy could lead to an unintentional loss of confidentiality.

NEW QUESTION 45

- (Topic 1)

An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

- A. Evidence collected through personal observation
- B. Evidence collected through systems logs provided by the organization's security administration
- C. Evidence collected through surveys collected from internal staff
- D. Evidence collected through transaction reports provided by the organization's IT administration

Answer: A

Explanation:

An IS auditor usually places more reliance on evidence directly collected, such as through personal observation.

NEW QUESTION 48

- (Topic 1)

Why does the IS auditor often review the system logs?

- A. To get evidence of password spoofing
- B. To get evidence of data copy activities
- C. To determine the existence of unauthorized access to data by a user or program
- D. To get evidence of password sharing

Answer: C

Explanation:

When trying to determine the existence of unauthorized access to data by a user or program, the IS auditor will often review the system logs.

NEW QUESTION 49

- (Topic 1)

What benefit does using capacity-monitoring software to monitor usage patterns and trends provide to management? Choose the BEST answer.

- A. The software can dynamically readjust network traffic capabilities based upon current usage
- B. The software produces nice reports that really impress management
- C. It allows users to properly allocate resources and ensure continuous efficiency of operation
- D. It allows management to properly allocate resources and ensure continuous efficiency of operation

Answer: D

Explanation:

Using capacity-monitoring software to monitor usage patterns and trends enables management to properly allocate resources and ensure continuous efficiency of operations.

NEW QUESTION 52

- (Topic 1)

What are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information? Choose the BEST answer.

- A. Referential integrity controls
- B. Normalization controls
- C. Concurrency controls
- D. Run-to-run totals

Answer: A

Explanation:

Concurrency controls are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information.

NEW QUESTION 55

- (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 59

- (Topic 1)

What is an initial step in creating a proper firewall policy?

- A. Assigning access to users according to the principle of least privilege
- B. Determining appropriate firewall hardware and software
- C. Identifying network applications such as mail, web, or FTP servers
- D. Configuring firewall access rules

Answer: C

Explanation:

Identifying network applications such as mail, web, or FTP servers to be externally accessed is an initial step in creating a proper firewall policy.

NEW QUESTION 60

- (Topic 1)

What type of cryptosystem is characterized by data being encrypted by the sender using the recipient's public key, and the data then being decrypted using the recipient's private key?

- A. With public-key encryption, or symmetric encryption
- B. With public-key encryption, or asymmetric encryption
- C. With shared-key encryption, or symmetric encryption
- D. With shared-key encryption, or asymmetric encryption

Answer: B

Explanation:

With public key encryption or asymmetric encryption, data is encrypted by the sender using the recipient's public key; the data is then decrypted using the recipient's private key.

NEW QUESTION 62

- (Topic 1)

Which of the following do digital signatures provide?

- A. Authentication and integrity of data
- B. Authentication and confidentiality of data
- C. Confidentiality and integrity of data
- D. Authentication and availability of data

Answer: A

Explanation:

The primary purpose of digital signatures is to provide authentication and integrity of data.

NEW QUESTION 66

- (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 key
- B. Upon receiving the data, the recipient can decrypt the data using the sender's public key
- C. A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public key
- D. Upon receiving the data, the recipient can decrypt the data using the recipient's public key
- 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 a hash value
- G. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public key
- H. Upon receiving the data, the recipient can decrypt the data using the recipient's private key

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 67

- (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 71

- (Topic 1)

Which of the following is an effective method for controlling downloading of files via FTP? Choose the BEST answer.

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

Answer: B

Explanation:

Application-layer gateways, or proxy firewalls, are an effective method for controlling downloading of files via FTP. Because FTP is an OSI application-layer protocol, the most effective firewall needs to be capable of inspecting through the application layer.

NEW QUESTION 72

- (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 77

- (Topic 1)

What is the key distinction between encryption and hashing algorithms?

- A. Hashing algorithms ensure data confidentiality
- B. Hashing algorithms are irreversible
- C. Encryption algorithms ensure data integrity
- D. Encryption algorithms are not irreversible

Answer: B

Explanation:

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

NEW QUESTION 81

- (Topic 1)

Which of the following is BEST characterized by unauthorized modification of data before or during systems data entry?

- A. Data diddling
- B. Skimming
- C. Data corruption
- D. Salami attack

Answer: A

Explanation:

Data diddling involves modifying data before or during systems data entry.

NEW QUESTION 83

- (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 84

- (Topic 1)

Who is ultimately responsible and accountable for reviewing user access to systems?

- A. Systems security administrators
- B. Data custodians
- C. Data owners
- D. Information systems auditors

Answer: C

Explanation:

Data owners are ultimately responsible and accountable for reviewing user access to systems.

NEW QUESTION 89

- (Topic 1)

Which of the following is MOST 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 90

- (Topic 1)

Which of the following typically focuses on making alternative processes and resources available for transaction processing?

- A. Cold-site facilities
- B. Disaster recovery for networks
- C. Diverse processing
- D. Disaster recovery for systems

Answer: D

Explanation:

Disaster recovery for systems typically focuses on making alternative processes and resources available for transaction processing.

NEW QUESTION 95

- (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-through
- 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 96

- (Topic 1)

What influences decisions regarding criticality of assets?

- A. The business criticality of the data to be protected
- B. Internal corporate politics
- C. The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole
- D. The business impact analysis

Answer: C

Explanation:

Criticality of assets is often influenced by the business criticality of the data to be protected and by the scope of the impact upon the organization as a whole. For example, the loss of a network backbone creates a much greater impact on the organization as a whole than the loss of data on a typical user's workstation.

NEW QUESTION 97

- (Topic 1)

Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following? Choose the BEST answer.

- A. IT strategic plan
- B. Business continuity plan
- C. Business impact analysis
- D. Incident response plan

Answer: B

Explanation:

Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of a business continuity plan.

NEW QUESTION 101

- (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 104

- (Topic 1)

Whenever an application is modified, what should be tested to determine the full impact of the change? Choose the BEST answer.

- A. Interface systems with other applications or systems
- B. The entire program, including any interface systems with other applications or systems
- C. All programs, including interface systems with other applications or systems
- D. Mission-critical functions and any interface systems with other applications or systems

Answer: B

Explanation:

Whenever an application is modified, the entire program, including any interface systems with other applications or systems, should be tested to determine the full impact of the change.

NEW QUESTION 106

- (Topic 1)

The quality of the metadata produced from a data warehouse is _____ in the warehouse's design. Choose the BEST answer.

- A. Often hard to determine because the data is derived from a heterogeneous data environment
- B. The most important consideration
- C. Independent of the quality of the warehoused databases
- D. Of secondary importance to data warehouse content

Answer: B

Explanation:

The quality of the metadata produced from a data warehouse is the most important consideration in the warehouse's design.

NEW QUESTION 107

- (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 111

- (Topic 1)

Run-to-run totals can verify data through which stage(s) of application processing?

- A. Initial
- B. Various
- C. Final
- D. Output

Answer: B

Explanation:

Run-to-run totals can verify data through various stages of application processing.

NEW QUESTION 112

- (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 117

- (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 120

- (Topic 1)

_____ risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a _____ risk assessment is more appropriate. Fill in the blanks.

- A. Quantitative; qualitative
- B. Qualitative; quantitative
- C. Residual; subjective
- D. Quantitative; subjective

Answer: A

Explanation:

Quantitative risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a qualitative risk assessment is more appropriate.

NEW QUESTION 122

- (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 125

- (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 130

- (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 134

- (Topic 1)

When are benchmarking partners identified within the benchmarking process?

- A. In the design stage
- B. In the testing stage
- C. In the research stage
- D. In the development stage

Answer: C

Explanation:

Benchmarking partners are identified in the research stage of the benchmarking process.

NEW QUESTION 138

- (Topic 1)

Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

- A. Proper authentication
- B. Proper identification AND authentication
- C. Proper identification
- D. Proper identification, authentication, AND authorization

Answer: B

Explanation:

If proper identification and authentication are not performed during access control, no accountability can exist for any action performed.

NEW QUESTION 140

- (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 145

- (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 150

- (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 153

- (Topic 1)

An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated data. True or false?

- A. True
- B. False

Answer: B

Explanation:

An integrated test facility is considered a useful audit tool because it compares processing output with independently calculated data.

NEW QUESTION 154

- (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 management
- B. To reassign job functions to eliminate potential fraud
- C. To implement compensating control
- D. Segregation of duties is an administrative control not considered by an IS auditor

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 159

- (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 161

- (Topic 1)

Ensuring that security and control policies support business and IT objectives is a primary objective of:

- A. An IT security policies audit
- B. A processing audit
- C. A software audit
- D. A vulnerability assessment

Answer: A

Explanation:

Ensuring that security and control policies support business and IT objectives is a primary objective of an IT security policies audit.

NEW QUESTION 166

- (Topic 1)

When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered. The auditor should especially focus on procedures in an audit of IS strategy. True or false?

- A. True
- B. False

Answer: B

Explanation:

When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered.

NEW QUESTION 168

- (Topic 1)

The directory system of a database-management system describes:

- A. The access method to the data
- B. The location of data AND the access method
- C. The location of data
- D. Neither the location of data NOR the access method

Answer: B

Explanation:

The directory system of a database-management system describes the location of data and the access method.

NEW QUESTION 170

- (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 175

- (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 177

- (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 178

- (Topic 1)

Which of the following help(s) prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack? Choose the BEST answer.

- A. Inbound traffic filtering
- B. Using access control lists (ACLs) to restrict inbound connection attempts
- C. Outbound traffic filtering
- D. Recentralizing distributed systems

Answer: C

Explanation:

Outbound traffic filtering can help prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack.

NEW QUESTION 180

- (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 183

- (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 187

- (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 190

- (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 191

- (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 195

- (Topic 1)

Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource? Choose the BEST answer.

- A. Systems logs
- B. Access control lists (ACL)
- C. Application logs
- D. Error logs

Answer: B

Explanation:

IS auditors should review access-control lists (ACL) to determine user permissions that have been granted for a particular resource.

NEW QUESTION 199

- (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 203

- (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 208

- (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 210

- (Topic 1)

Rather than simply reviewing the adequacy of access control, appropriateness of access policies, and effectiveness of safeguards and procedures, the IS auditor is more concerned with effectiveness and utilization of assets. True or false?

- A. True
- B. False

Answer: B

Explanation:

Instead of simply reviewing the effectiveness and utilization of assets, an IS auditor is more concerned with adequate access control, appropriate access policies, and effectiveness of safeguards and procedures.

NEW QUESTION 212

- (Topic 1)

How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

- A. By implementing redundant systems and applications onsite
- B. By geographically dispersing resources
- C. By retaining onsite data backup in fireproof vaults
- D. By preparing BCP and DRP documents for commonly identified disasters

Answer: B

Explanation:

Minimizing single points of failure or vulnerabilities of a common disaster is mitigated by geographically dispersing resources.

NEW QUESTION 217

- (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 220

- (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 225

- (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 230

- (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 232

- (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 233

- (Topic 1)

When should application controls be considered within the system-development process?

- A. After application unit testing
- B. After application module testing
- C. After applications systems testing
- D. As early as possible, even in the development of the project's functional specifications

Answer: D

Explanation:

Application controls should be considered as early as possible in the system-development process, even in the development of the project's functional specifications.

NEW QUESTION 236

- (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 239

- (Topic 1)

Who is responsible for the overall direction, costs, and timetables for systems-development projects?

- A. The project sponsor
- B. The project steering committee
- C. Senior management
- D. The project team leader

Answer: B

Explanation:

The project steering committee is responsible for the overall direction, costs, and timetables for systems-development projects.

NEW QUESTION 241

- (Topic 1)

Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

- A. Failing to perform user acceptance testing
- B. Lack of user training for the new system
- C. Lack of software documentation and run manuals
- D. Insufficient unit, module, and systems testing

Answer: A

Explanation:

Above almost all other concerns, failing to perform user acceptance testing often results in the greatest negative impact on the implementation of new application software.

NEW QUESTION 246

- (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 248

- (Topic 1)

After identifying potential security vulnerabilities, what should be the IS auditor's next step?

- A. To evaluate potential countermeasures and compensatory controls
- B. To implement effective countermeasures and compensatory controls
- C. To perform a business impact analysis of the threats that would exploit the vulnerabilities
- D. To immediately advise senior management of the findings

Answer: C

Explanation:

After identifying potential security vulnerabilities, the IS auditor's next step is to perform a business impact analysis of the threats that would exploit the vulnerabilities.

NEW QUESTION 251

- (Topic 1)

_____ (fill in the blank) should be implemented as early as data preparation to support data integrity at the earliest point possible.

- A. Control totals
- B. Authentication controls
- C. Parity bits
- D. Authorization controls

Answer: A

Explanation:

Control totals should be implemented as early as data preparation to support data integrity at the earliest point possible.

NEW QUESTION 256

- (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 261

- (Topic 1)

Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

- A. True
- B. False

Answer: A

Explanation:

Database snapshots can provide an excellent audit trail for an IS auditor.

NEW QUESTION 264

- (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 269

- (Topic 2)

Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

- A. Multiple cycles of backup files remain available
- B. Access controls establish accountability for e-mail activities
- C. Data classification regulates what information should be communicated via e-mail
- D. Within the enterprise, a clear policy for using e-mail ensures that evidence is available

Answer: A

Explanation:

Backup files containing documents that supposedly have been deleted could be recovered from these files. Access controls may help establish accountability for the issuance of a particular document, but this does not provide evidence of the e-mail. Data classification standards may be in place with regards to what should be communicated via e-mail, but the creation of the policy does not provide the information required for litigation purposes.

NEW QUESTION 271

- (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 audit
- B. train the IS audit staff on current technology used in the company
- C. develop the audit plan on the basis of a detailed risk assessment
- D. monitor progress of audits and initiate cost control measures

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 273

- (Topic 2)

An organization's IS audit charter should specify the:

- A. short- and long-term plans for IS audit engagements
- B. objectives and scope of IS audit engagement
- C. detailed training plan for the IS audit staff
- D. role of the IS audit function

Answer: D

Explanation:

An IS audit charter establishes the role of the information systems audit function. The charter should describe the overall authority, scope, and responsibilities of the audit function. It should be approved by the highest level of management and, if available, by the audit committee. Short-term and long-term planning is the responsibility of audit management. The objectives and scope of each IS audit should be agreed to in an engagement letter. A training plan, based on the audit plan, should be developed by audit management.

NEW QUESTION 274

- (Topic 2)

An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

- A. the probability of error must be objectively quantified
- B. the auditor wishes to avoid sampling risk
- C. generalized audit software is unavailable
- D. the tolerable error rate cannot be determined

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 277

- (Topic 2)

During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

- A. address audit objectives
- B. collect sufficient evidence
- C. specify appropriate tests
- D. minimize audit resources

Answer: A

Explanation:

ISACA auditing standards require that an IS auditor plan the audit work to address the audit objectives. Choice B is incorrect because the auditor does not collect evidence in the planning stage of an audit. Choices C and D are incorrect because they are not the primary goals of audit planning. The activities described in choices B, C and D are all undertaken to address audit objectives and are thus secondary to choice A.

NEW QUESTION 280

- (Topic 2)

An IS auditor evaluating logical access controls should FIRST:

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

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 and evaluation 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, the IS 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 283

- (Topic 2)

The PRIMARY purpose of an IT forensic audit is:

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

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 287

- (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 network
- B. Users can install software on their desktop
- C. Network monitoring is very limited
- D. Many user IDs have identical passwords

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 detect abuse of user accounts in special circumstances and is, therefore, not a first line of defense.

NEW QUESTION 290

CORRECT TEXT - (Topic 2)

The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

- A. Test data
- B. Generalized audit software
- C. Integrated test facility
- D. Embedded audit module

Answer: B

NEW QUESTION 294

- (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 298

- (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 observations and 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 regarding segregation 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 302

- (Topic 2)

An IS auditor reviews an organizational chart PRIMARILY for:

- A. an understanding of workflow
- B. investigating various communication channel
- C. understanding the responsibilities and authority of individual
- D. investigating the network connected to different employee

Answer: C

Explanation:

An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps an IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

NEW QUESTION 305

- (Topic 2)

An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

- A. evaluate the record retention plans for off-premises storage
- B. interview programmers about the procedures currently being followed
- C. compare utilization records to operations schedule
- D. review data file access records to test the librarian function

Answer: B

Explanation:

Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests the recovery procedures, not the access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

NEW QUESTION 307

- (Topic 2)

In an audit of an inventory application, which approach would provide the BEST evidence that purchase orders are valid?

- A. Testing whether inappropriate personnel can change application parameters
- B. Tracing purchase orders to a computer listing
- C. Comparing receiving reports to purchase order details
- D. Reviewing the application documentation

Answer: A

Explanation:

To determine purchase order validity, testing access controls will provide the best evidence. Choices B and C are based on after-the-fact approaches, while choice D does not serve the purpose because what is in the system documentation may not be the same as what is happening.

NEW QUESTION 308

- (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 audit trail is required.

NEW QUESTION 313

- (Topic 2)

When assessing the design of network monitoring controls, an IS auditor should FIRST review network:

- A. topology diagram
- B. bandwidth usage
- C. traffic analysis report
- D. bottleneck location

Answer: A

Explanation:

The first step in assessing network monitoring controls should be the review of the adequacy of network documentation, specifically topology diagrams. If this information is not up to date, then monitoring processes and the ability to diagnose problems will not be effective.

NEW QUESTION 316

- (Topic 2)

While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?

- A. Observe the response mechanism
- B. Clear the virus from the network
- C. Inform appropriate personnel immediately
- D. Ensure deletion of the virus

Answer: C

Explanation:

The first thing an IS auditor should do after detecting the virus is to alert the organization to its presence, then wait for their response. Choice A should be taken after choice C. This will enable an IS auditor to examine the actual workability and effectiveness of the response system. An IS auditor should not make changes to the system being audited, and ensuring the deletion of the virus is a management responsibility.

NEW QUESTION 321

- (Topic 2)

A substantive test to verify that tape library inventory records are accurate is:

- A. determining whether bar code readers are installed
- B. determining whether the movement of tapes is authorized
- C. conducting a physical count of the tape inventory
- D. checking if receipts and issues of tapes are accurately recorded

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 325

- (Topic 2)

While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

- A. audit trail of the versioning of the work paper
- B. approval of the audit phase
- C. access rights to the work paper
- D. confidentiality of the work paper

Answer: D

Explanation:

Encryption provides confidentiality for the electronic work papers. Audit trails, audit phase approvals and access to the work papers do not, of themselves, affect the confidentiality but are part of the reason for requiring encryption.

NEW QUESTION 326

- (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 warranted
- B. report the matter to the audit committee
- C. report the possibility of fraud to top management and ask how they would like to proceed
- D. consult with external legal counsel to determine the course of action to be taken

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 327

- (Topic 2)

During a change control audit of a production system, an IS auditor finds that the change management process is not formally documented and that some migration procedures failed. What should the IS auditor do next?

- A. Recommend redesigning the change management process
- B. Gain more assurance on the findings through root cause analysis
- C. Recommend that program migration be stopped until the change process is documented
- D. Document the finding and present it to management

Answer: B

Explanation:

A change management process is critical to IT production systems. Before recommending that the organization take any other action (e.g., stopping migrations, redesigning the change management process), the IS auditor should gain assurance that the incidents reported are related to deficiencies in the change management process and not caused by some process other than change management.

NEW QUESTION 331

- (Topic 2)

An IS auditor who was involved in designing an organization's business continuity plan (BCP) has been assigned to audit the plan. The IS auditor should:

- A. decline the assignment
- B. inform management of the possible conflict of interest after completing the audit assignment
- C. inform the business continuity planning (BCP) team of the possible conflict of interest prior to beginning the assignment
- D. communicate the possibility of conflict of interest to management prior to starting the assignment

Answer: D

Explanation:

Communicating the possibility of a conflict of interest to management prior to starting the assignment is the correct answer. A possible conflict of interest, likely to affect the auditor's independence, should be brought to the attention of management prior to starting the assignment. Declining the assignment is not the correct answer because the assignment could be accepted after obtaining management approval. Informing management of the possible conflict of interest after completion of the audit assignment is not correct because approval should be obtained prior to commencement and not after the completion of the assignment. Informing the business continuity planning (BCP) team of the possible conflict of interest prior to starting of the assignment is not the correct answer since the BCP team would not have the authority to decide on this issue.

NEW QUESTION 332

- (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 software
- B. Inform the auditee of the unauthorized software, and follow up to confirm deletion
- C. Report the use of the unauthorized software and the need to prevent recurrence to auditee management
- D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use

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 335

- (Topic 2)

Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:

- A. include the finding in the final report, because the IS auditor is responsible for an accurate report of all finding
- B. not include the finding in the final report, because the audit report should include only unresolved finding
- C. not include the finding in the final report, because corrective action can be verified by the IS auditor during the audi
- D. include the finding in the closing meeting for discussion purposes onl

Answer: A

Explanation:

Including the finding in the final report is a generally accepted audit practice. If an action is taken after the audit started and before it ended, the audit report should identify the finding and describe the corrective action taken. An audit report should reflect the situation, as it existed at the start of the audit. All corrective actions taken by the auditee should be reported in writing.

NEW QUESTION 337

- (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 341

- (Topic 2)

During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:

- A. ask the auditee to sign a release form accepting full legal responsibilit
- B. elaborate on the significance of the finding and the risks of not correcting i
- C. report the disagreement to the audit committee for resolutio
- D. accept the auditee's position since they are the process owner

Answer: B

Explanation:

If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risks and exposures, as the auditee may not fully appreciate the magnitude of the exposure. The goal should be to enlighten the auditee or uncover new information of which an IS auditor may not have been aware. Anything that appears to threaten the auditee will lessen effective communications and set up an adversarial relationship. By the same token, an IS auditor should not automatically agree just because the auditee expresses an alternate point of view.

NEW QUESTION 344

- (Topic 2)

When preparing an audit report the IS auditor should ensure that the results are supported by:

- A. statements from IS managemen
- B. workpapers of other auditor
- C. an organizational control self-assessmen
- D. sufficient and appropriate audit evidenc

Answer: D

Explanation:

ISACA's standard on 'reporting' requires the IS auditor have sufficient and appropriate audit evidence to support the reported results. Statements from IS management provide a basis for obtaining concurrence on matters that cannot be verified with empirical evidence. The report should be based on evidence collected during the course of the review even though the auditor may have access to the work papers of other auditors. The results of an organizational control self-assessment (CSA) could supplement the audit findings. Choices A, B and C might be referenced during an audit but, of themselves, would not be considered a sufficient basis for issuing a report.

NEW QUESTION 348

- (Topic 2)

Which of the following is an attribute of the control self-assessment (CSA) approach?

- A. Broad stakeholder involvement
- B. Auditors are the primary control analysts
- C. Limited employee participation
- D. Policy driven

Answer: A

Explanation:

The control self-assessment (CSA) approach emphasizes management of and accountability for developing and monitoring the controls of an organization's business processes. The attributes of CSA include empowered employees, continuous improvement, extensive employee participation and training, all of which are representations of broad stakeholder involvement. Choices B, C and D are attributes of a traditional audit approach.

NEW QUESTION 349

- (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 reinforced
- B. Audit expenses are reduced when the assessment results are an input to external audit work
- 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 assessments

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 354

- (Topic 3)

The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

- A. a lack of investment in technology
- B. a lack of a methodology for systems development
- 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 356

- (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 361

- (Topic 3)

An IS steering committee should:

- A. include a mix of members from different departments and staff level
- B. ensure that IS security policies and procedures have been executed properly
- C. have formal terms of reference and maintain minutes of its meeting
- D. be briefed about new trends and products at each meeting by a vendor

Answer: C

Explanation:

It is important to keep detailed steering committee minutes to document the decisions and activities of the IS steering committee, and the board of directors should be informed about those decisions on a timely basis. Choice A is incorrect because only senior management or high-level staff members should be on this committee because of its strategic mission. Choice B is not a responsibility of this committee, but the responsibility of the security administrator. Choice D is incorrect because a vendor should be invited to meetings only when appropriate.

NEW QUESTION 364

- (Topic 3)

IT governance is PRIMARILY the responsibility of the:

- A. chief executive office
- B. board of director
- C. IT steering committee
- D. audit committee

Answer: B

Explanation:

IT governance is primarily the responsibility of the executives and shareholders (as represented by the board of directors). The chief executive officer is instrumental in implementing IT governance per the directions of the board of directors. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. The audit committee reports to the board of directors and should monitor the implementation of audit recommendations.

NEW QUESTION 367

- (Topic 3)

When implementing an IT governance framework in an organization the MOST important objective is:

- A. IT alignment with the business
- B. accountability
- C. value realization with IT
- D. enhancing the return on IT investment

Answer: A

Explanation:

The goals of IT governance are to improve IT performance, to deliver optimum business value and to ensure regulatory compliance. The key practice in support of these goals is the strategic alignment of IT with the business (choice A). To achieve alignment, all other choices need to be tied to business practices and strategies.

NEW QUESTION 372

- (Topic 3)

The ultimate purpose of IT governance is to:

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

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 373

- (Topic 3)

Responsibility for the governance of IT should rest with the:

- A. IT strategy committee
- B. chief information officer (CIO).
- C. audit committee
- 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 375

- (Topic 3)

An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

- A. User acceptance testing (UAT) occur for all reports before release into production
- B. Organizational data governance practices be put in place
- C. Standard software tools be used for report development
- D. Management sign-off on requirements for new reports

Answer: B

Explanation:

This choice directly addresses the problem. An organizationwide approach is needed to achieve effective management of data assets. This includes enforcing standard definitions of data elements, which is part of a data governance initiative. The other choices, while sound development practices, do not address the root cause of the problem described.

NEW QUESTION 380

- (Topic 3)

Which of the following would BEST provide assurance of the integrity of new staff?

- A. Background screening
- B. References
- C. Bonding
- D. Qualifications listed on a resume

Answer: A

Explanation:

A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a resume may not be accurate.

NEW QUESTION 384

- (Topic 3)

When an employee is terminated from service, the MOST important action is to:

- A. hand over all of the employee's files to another designated employee
- B. complete a backup of the employee's work
- C. notify other employees of the termination
- D. disable the employee's logical access

Answer: D

Explanation:

There is a probability that a terminated employee may misuse access rights; therefore, disabling the terminated employee's logical access is the most important action to take. All the work of the terminated employee needs to be handed over to a designated employee; however, this should be performed after implementing choice D. All the work of the terminated employee needs to be backed up and the employees need to be notified of the termination of the employee, but this should not precede the action in choice D.

NEW QUESTION 388

- (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 productivity
- B. reduce the opportunity for an employee to commit an improper or illegal act
- C. provide proper cross-training for another employee
- D. eliminate the potential disruption caused when an employee takes vacation one day at a time

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 393

- (Topic 3)

A local area network (LAN) administrator normally would be restricted from:

- A. having end-user responsibilities
- B. reporting to the end-user manager
- C. having programming responsibilities
- D. being responsible for LAN security administration

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 396

- (Topic 3)

A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual's experience and:

- A. length of service, since this will help ensure technical competency
- B. age, as training in audit techniques may be impractical
- C. IS knowledge, since this will bring enhanced credibility to the audit function
- D. ability, as an IS auditor, to be independent of existing IS relationships

Answer: D

Explanation:

Independence should be continually assessed by the auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities. The fact that the employee has worked in IS for many years may not in itself ensure credibility. The audit department's needs should be defined and any candidate should be evaluated against those requirements. The length of service will not ensure technical competency. Evaluating an individual's qualifications based on the age of the individual is not a good criterion and is illegal in many parts of the world.

NEW QUESTION 400

- (Topic 3)

An IS auditor should be concerned when a telecommunication analyst:

- A. monitors systems performance and tracks problems resulting from program change
- B. reviews network load requirements in terms of current and future transaction volume
- C. assesses the impact of the network load on terminal response times and network data transfer rate
- D. recommends network balancing procedures and improvement

Answer: A

Explanation:

The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes (choice B), assessing the impact of network load or terminal response times and network data transfer rates (choice C), and recommending network balancing procedures and improvements (choice D). Monitoring systems performance and tracking problems as a result of program changes (choice A) would put the analyst in a self-monitoring role.

NEW QUESTION 404

- (Topic 3)

An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

- A. dependency on a single person
- B. inadequate succession planning
- C. one person knowing all parts of a system
- D. a disruption of operation

Answer: C

Explanation:

Cross-training is a process of training more than one individual to perform a specific job or procedure. This practice helps decrease the dependence on a single person and assists in succession planning. This provides for the backup of personnel in the event of an absence and, thereby, provides for the continuity of operations. However, in using this approach, it is prudent to have first assessed the risk of any person knowing all parts of a system and the related potential exposures. Cross-training reduces the risks addressed in choices A, B and D.

NEW QUESTION 406

- (Topic 3)

Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

- A. Overlapping controls
- B. Boundary controls
- C. Access controls
- D. Compensating controls

Answer: D

Explanation:

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness that may arise when duties cannot be

appropriately segregated. Overlapping controls are two controls addressing the same control objective or exposure. Since primary controls cannot be achieved when duties cannot or are not appropriately segregated, it is difficult to install overlapping controls. Boundary controls establish the interface between the would-be user of a computer system and the computer system itself, and are individual-based, not role-based, controls. Access controls for resources are based on individuals and not on roles.

NEW QUESTION 407

- (Topic 3)

Which of the following reduces the potential impact of social engineering attacks?

- A. Compliance with regulatory requirements
- B. Promoting ethical understanding
- C. Security awareness programs
- D. Effective performance incentives

Answer: C

Explanation:

Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

NEW QUESTION 411

- (Topic 3)

Which of the following is a risk of cross-training?

- A. Increases the dependence on one employee
- B. Does not assist in succession planning
- C. One employee may know all parts of a system
- D. Does not help in achieving a continuity of operations

Answer: C

Explanation:

When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

NEW QUESTION 414

- (Topic 3)

Which of the following is normally a responsibility of the chief security officer (CSO)?

- A. Periodically reviewing and evaluating the security policy
- B. Executing user application and software testing and evaluation
- C. Granting and revoking user access to IT resources
- D. Approving access to data and applications

Answer: A

Explanation:

The role of a chief security officer (CSO) is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the company assets, including data, programs and equipment. User application and other software testing and evaluation normally are the responsibility of the staff assigned to development and maintenance. Granting and revoking access to IT resources is usually a function of network or database administrators. Approval of access to data and applications is the duty of the data owner.

NEW QUESTION 419

- (Topic 3)

Which of the following goals would you expect to find in an organization's strategic plan?

- A. Test a new accounting packag
- B. Perform an evaluation of information technology need
- C. Implement a new project planning system within the next 12 month
- D. Become the supplier of choice for the product offere

Answer: D

Explanation:

Strategic planning sets corporate or departmental objectives into motion. Comprehensive planning helps ensure an effective and efficient organization. Strategic planning is time-and project-oriented, but also must address and help determine priorities to meet business needs. Long- and short-range plans should be consistent with the organization's broader plans for attaining their goals. Choice D represents a business objective that is intended to focus the overall direction of the business and would thus be a part of the organization's strategic plan. The other choices are project-oriented and do not address business objectives.

NEW QUESTION 424

- (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 429

- (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 costs
- C. a listing of approved suppliers of IT contract resource
- D. a description of the technical architecture for the organization's network perimeter security

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 to set 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 of a specific technical architecture.

NEW QUESTION 430

- (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 whole
- B. are more likely to be derived as a result of a risk assessment
- C. will not conflict with overall corporate policy
- D. ensure consistency across the organization

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 431

- (Topic 3)

Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

- A. User management coordination does not exist
- B. Specific user accountability cannot be established
- C. Unauthorized users may have access to originate, modify or delete data
- D. Audit recommendations may not be implemented

Answer: C

Explanation:

Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

NEW QUESTION 434

- (Topic 3)

The PRIMARY objective of an audit of IT security policies is to ensure that:

- A. they are distributed and available to all staff
- B. security and control policies support business and IT objectives
- C. there is a published organizational chart with functional descriptions
- D. duties are appropriately segregated

Answer: B

Explanation:

Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives. Reviewing whether policies are available to all is an objective, but distribution does not ensure compliance. Availability of organizational charts with functional descriptions and segregation of duties might be included in the review, but are not the primary objective of an audit of security policies.

NEW QUESTION 437

- (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 official form 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 439

- (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 444

- (Topic 3)

To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

- A. the IT infrastructur
- B. organizational policies, standards and procedure
- C. legal and regulatory requirement
- D. the adherence to organizational policies, standards and procedure

Answer: C

Explanation:

To ensure that the organization is complying with privacy issues, an IS auditor should address legal and regulatory requirements first. To comply with legal and regulatory requirements, organizations need to adopt the appropriate infrastructure. After understanding the legal and regulatory requirements, an IS auditor should evaluate organizational policies, standards and procedures to determine whether they adequately address the privacy requirements, and then review the adherence to these specific policies, standards and procedures.

NEW QUESTION 445

- (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 periodical

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 449

- (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 year
- C. Privacy laws could prevent cross-border flow of information
- 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 454

- (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 455

- (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 will often 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 459

- (Topic 3)

The initial step in establishing an information security program is the:

- A. development and implementation of an information security standards manual
- B. performance of a comprehensive security control review by the IS auditor
- C. adoption of a corporate information security policy statement
- D. purchase of security access control software

Answer: C

Explanation:

A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

NEW QUESTION 463

- (Topic 3)

Which of the following provides the best evidence of the adequacy of a security awareness program?

- A. The number of stakeholders including employees trained at various levels
- B. Coverage of training at all locations across the enterprise
- C. The implementation of security devices from different vendors
- D. Periodic reviews and comparison with best practices

Answer: D

Explanation:

The adequacy of security awareness content can best be assessed by determining whether it is periodically reviewed and compared to industry best practices. Choices A, B and C provide metrics for measuring various aspects of a security awareness program, but do not help assess the content.

NEW QUESTION 464

- (Topic 3)

The PRIMARY objective of implementing corporate governance by an organization's management is to:

- A. provide strategic direction
- B. control business operation
- C. align IT with business
- D. implement best practice

Answer: A

Explanation:

Corporate governance is a set of management practices to provide strategic direction, thereby ensuring that goals are achievable, risks are properly addressed and organizational resources are properly utilized. Hence, the primary objective of corporate governance is to provide strategic direction. Based on the strategic direction, business operations are directed and controlled.

NEW QUESTION 466

- (Topic 3)

An example of a direct benefit to be derived from a proposed IT-related business investment is:

- A. enhanced reputation
- B. enhanced staff morale
- C. the use of new technology
- D. increased market penetration

Answer: D

Explanation:

A comprehensive business case for any proposed IT-related business investment should have clearly defined business benefits to enable the expected return to be calculated. These benefits usually fall into two categories: direct and indirect, or soft. Direct benefits usually comprise the quantifiable financial benefits that the new system is expected to generate. The potential benefits of enhanced reputation and enhanced staff morale are difficult to quantify, but should be quantified to the extent possible. IT investments should not be made just for the sake of new technology but should be based on a quantifiable business need.

NEW QUESTION 470

- (Topic 3)

A benefit of open system architecture is that it:

- A. facilitates interoperability
- B. facilitates the integration of proprietary components
- C. will be a basis for volume discounts from equipment vendors
- D. allows for the achievement of more economies of scale for equipment

Answer: A

Explanation:

Open systems are those for which suppliers provide components whose interfaces are defined by public standards, thus facilitating interoperability between systems made by different vendors. In contrast, closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems.

NEW QUESTION 475

- (Topic 3)

In the context of effective information security governance, the primary objective of value delivery is to:

- A. optimize security investments in support of business objectives
- B. implement a standard set of security practices
- C. institute a standards-based solution
- D. implement a continuous improvement culture

Answer: A

Explanation:

In the context of effective information security governance, value delivery is implemented to ensure optimization of security investments in support of business objectives. The tools and techniques for implementing value delivery include implementation of a standard set of security practices, institutionalization and commoditization of standards-based solutions, and implementation of a continuous improvement culture considering security as a process, not an event.

NEW QUESTION 476

- (Topic 3)

When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

- A. There could be a question regarding the legal jurisdiction
- B. Having a provider abroad will cause excessive costs in future audit
- C. The auditing process will be difficult because of the distance
- D. There could be different auditing norms

Answer: A

Explanation:

In the funds transfer process, when the processing scheme is centralized in a different country, there could be legal issues of jurisdiction that might affect the right to perform a review in the other country. The other choices, though possible, are not as relevant as the issue of legal jurisdiction.

NEW QUESTION 480

- (Topic 3)

An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

- A. References from other customers
- B. Service level agreement (SLA) template
- C. Maintenance agreement
- D. Conversion plan

Answer: A

Explanation:

An IS auditor should look for an independent verification that the ISP can perform the tasks being contracted for. References from other customers would provide an independent, external review and verification of procedures and processes the ISP follows—issues which would be of concern to an IS auditor. Checking references is a means of obtaining an independent verification that the vendor can perform the services it says it can. A maintenance agreement relates more to equipment than to services, and a conversion plan, while important, is less important than verification that the ISP can provide the services they propose.

NEW QUESTION 485

- (Topic 3)

To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

- A. O/S and hardware refresh frequencies
- B. Gain-sharing performance bonuses
- C. Penalties for noncompliance
- D. Charges tied to variable cost metrics

Answer: B

Explanation:

Because the outsourcer will share a percentage of the achieved savings, gain-sharing performance bonuses provide a financial incentive to go above and beyond the stated terms of the contract and can lead to cost savings for the client. Refresh frequencies and penalties for noncompliance would only encourage the outsourcer to meet minimum requirements. Similarly, tying charges to variable cost metrics would not encourage the outsourcer to seek additional efficiencies that might benefit the client.

NEW QUESTION 488

- (Topic 3)

With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?

- A. Outsourced activities are core and provide a differentiated advantage to the organization
- B. Periodic renegotiation is specified in the outsourcing contract
- C. The outsourcing contract fails to cover every action required by the arrangement
- D. Similar activities are outsourced to more than one vendor

Answer: A

Explanation:

An organization's core activities generally should not be outsourced, because they are what the organization does best; an IS auditor observing that should be concerned. An IS auditor should not be concerned about the other conditions because specification of periodic renegotiation in the outsourcing contract is a best practice. Outsourcing contracts cannot be expected to cover every action and detail expected of the parties involved, while multisourcing is an acceptable way to reduce risk.

NEW QUESTION 490

- (Topic 3)

Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

- A. meets or exceeds industry security standard
- B. agrees to be subject to external security review
- C. has a good market reputation for service and experience
- D. complies with security policies of the organization

Answer: B

Explanation:

It is critical that an independent security review of an outsourcing vendor be obtained because customer credit information will be kept there. Compliance with security standards or organization policies is important, but there is no way to verify or prove that that is the case without an independent review. Though long experience in business and good reputation is an important factor to assess service quality, the business cannot outsource to a provider whose security control is weak.

NEW QUESTION 494

- (Topic 3)

The risks associated with electronic evidence gathering would MOST likely be reduced by an e-mail:

- A. destruction polic
- B. security polic
- C. archive polic
- D. audit polic

Answer: C

Explanation:

With a policy of well-archived e-mail records, access to or retrieval of specific e-mail records is possible without disclosing other confidential e-mail records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying e-mails may be an illegal act.

NEW QUESTION 496

- (Topic 3)

The output of the risk management process is an input for making:

- A. business plan
- B. audit charter
- C. security policy decision
- D. software design decision

Answer: C

Explanation:

The risk management process is about making specific, security-related decisions, such as the level of acceptable risk. Choices A, B and D are not ultimate goals of the risk management process.

NEW QUESTION 497

- (Topic 3)

An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

- A. Report the risks to the CIO and CEO immediately
- B. Examine e-business application in development
- C. Identify threats and likelihood of occurrence
- D. Check the budget available for risk management

Answer: C

Explanation:

An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

NEW QUESTION 502

- (Topic 3)

When developing a risk management program, what is the FIRST activity to be performed?

- A. Threat assessment
- B. Classification of data
- C. Inventory of assets
- D. Criticality analysis

Answer: C

Explanation:

Identification of the assets to be protected is the first step in the development of a risk management program. A listing of the threats that can affect the performance of these assets and criticality analysis are later steps in the process. Data classification is required for defining access controls and in criticality analysis.

NEW QUESTION 506

- (Topic 3)

Which of the following does a lack of adequate security controls represent?

- A. Threat
- B. Asset
- C. Impact
- D. Vulnerability

Answer: D

Explanation:

The lack of adequate security controls represents a vulnerability, exposing sensitive information and data to the risk of malicious damage, attack or unauthorized access by hackers. This could result in a loss of sensitive information and lead to the loss of goodwill for the organization. A succinct definition of risk is provided by the Guidelines for the Management of IT Security published by the International Organization for Standardization (ISO), which defines risk as the 'potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.' The various elements of the definition are vulnerability, threat, asset and impact. Lack of adequate security functionality in this context is a vulnerability.

NEW QUESTION 509

- (Topic 3)

Assessing IT risks is BEST achieved by:

- A. evaluating threats associated with existing IT assets and IT project
- B. using the firm's past actual loss experience to determine current exposure
- C. reviewing published loss statistics from comparable organization
- D. reviewing IT control weaknesses identified in audit report

Answer: A

Explanation:

To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves are not sufficient. Basing an assessment on past losses will not adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to be assessed. Comparable organizations will have differences in their IT assets, control environment and strategic circumstances. Therefore, their loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not all of the critical IT assets and projects will have recently been audited, and there may not be a sufficient assessment of strategic IT risks.

NEW QUESTION 511

- (Topic 3)

A poor choice of passwords and transmission over unprotected communications lines are examples of:

- A. vulnerability
- B. threat
- C. probability
- D. impact

Answer: A

Explanation:

Vulnerabilities represent characteristics of information resources that may be exploited by a threat. Threats are circumstances or events with the potential to cause harm to information resources. Probabilities represent the likelihood of the occurrence of a threat, while impacts represent the outcome or result of a threat exploiting a vulnerability.

NEW QUESTION 516

- (Topic 3)

Which of the following should be considered FIRST when implementing a risk management program?

- A. An understanding of the organization's threat, vulnerability and risk profile
- B. An understanding of the risk exposures and the potential consequences of compromise
- C. A determination of risk management priorities based on potential consequences
- D. A risk mitigation strategy sufficient to keep risk consequences at an acceptable level

Answer: A

Explanation:

Implementing risk management, as one of the outcomes of effective information security governance, would require a collective understanding of the organization's threat, vulnerability and risk profile as a first step. Based on this, an understanding of risk exposure and potential consequences of compromise could be determined. Risk management priorities based on potential consequences could then be developed. This would provide a basis for the formulation of strategies for risk mitigation sufficient to keep the consequences from risk at an acceptable level.

NEW QUESTION 519

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISA Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISA Product From:

<https://www.2passeasy.com/dumps/CISA/>

Money Back Guarantee

CISA Practice Exam Features:

- * CISA Questions and Answers Updated Frequently
- * CISA Practice Questions Verified by Expert Senior Certified Staff
- * CISA Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CISA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year