

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)

Which of the following data validation edits is effective in detecting transposition and transcription errors?

- A. Range check
- B. Check digit
- C. Validity check
- D. Duplicate check

Answer: B

Explanation:

A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted. This control is effective in detecting transposition and transcription errors.

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)

A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

- A. Unit testing
- B. Integration testing
- C. Design walk-throughs
- D. Configuration management

Answer: B

Explanation:

A common system maintenance problem is that errors are often corrected quickly (especially when deadlines are tight), units are tested by the programmer, and then transferred to the acceptance test area. This often results in system problems that should have been detected during integration or system testing. Integration testing aims at ensuring that the major components of the system interface correctly.

NEW QUESTION 6

- (Topic 1)

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

- A. communications handle
- B. EDI translator
- C. application interface
- D. EDI interface

Answer: A

Explanation:

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

NEW QUESTION 7

- (Topic 1)

Which of the following network configuration options contains a direct link between any two host machines?

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

Answer: D

Explanation:

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

NEW QUESTION 8

- (Topic 1)

A data administrator is responsible for:

- A. maintaining database system software
- B. defining data elements, data names and their relationships
- C. developing physical database structure
- D. developing data dictionary system software

Answer: B

Explanation:

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

NEW QUESTION 9

- (Topic 1)

A database administrator is responsible for:

- A. defining data ownership
- B. establishing operational standards for the data dictionary
- C. creating the logical and physical databases
- D. establishing ground rules for ensuring data integrity and security

Answer: C

Explanation:

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

NEW QUESTION 10

- (Topic 1)

An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

- A. defining the conceptual schema
- B. defining security and integrity checks
- C. liaising with users in developing data models

D. mapping data model with the internal schem

Answer: D

Explanation:

A DBA only in rare instances should be mapping data elements from the data model to the internal schema (physical data storage definitions). To do so would eliminate data independence for application systems. Mapping of the data model occurs with the conceptual schema since the conceptual schema represents the enterprisewide view of data within an organization and is the basis for deriving an end-user department data model.

NEW QUESTION 10

- (Topic 1)

A critical function of a firewall is to act as a:

- A. special router that connects the Internet to a LA
- B. device for preventing authorized users from accessing the LA
- C. server used to connect authorized users to private trusted network resource
- D. proxy server to increase the speed of access to authorized user

Answer: B

Explanation:

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users of other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling the outside resources to which its own users have access. Basically, a firewall, working closely with a router program, filters all network packets to determine whether or not to forward them toward their destination. A firewall includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so no incoming request can get directed to private network resources.

NEW QUESTION 12

- (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 16

- (Topic 1)

The use of a GANTT chart can:

- A. aid in scheduling project task
- B. determine project checkpoint
- C. ensure documentation standard
- D. direct the post-implementation review

Answer: A

Explanation:

A GANTT chart is used in project control. It may aid in the identification of needed checkpoints but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post-implementation review.

NEW QUESTION 17

- (Topic 1)

Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

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

Answer: C

Explanation:

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

NEW QUESTION 22

- (Topic 1)

A hub is a device that connects:

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

Answer: D

Explanation:

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

NEW QUESTION 26

- (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 31

- (Topic 1)

For which of the following applications would rapid recovery be MOST crucial?

- A. Point-of-sale system
- B. Corporate planning
- C. Regulatory reporting
- D. Departmental chargeback

Answer: A

Explanation:

A point-of-sale system is a critical online system that when inoperable will jeopardize the ability of Company.com to generate revenue and track inventory properly.

NEW QUESTION 33

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 36

- (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 implementatio
- 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 40

- (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 authorit

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 41

- (Topic 1)

Which of the following is a data validation edit and control?

- A. Hash totals
- B. Reasonableness checks
- C. Online access controls
- D. Before and after image reporting

Answer: B

Explanation:

A reasonableness check is a data validation edit and control, used to ensure that data conforms to predetermined criteria.

NEW QUESTION 46

- (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 47

- (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 50

- (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 53

- (Topic 1)

Proper segregation of duties normally does not prohibit a LAN administrator from also having programming responsibilities. True or false?

- A. True
- B. False

Answer: B

Explanation:

Proper segregation of duties normally prohibits a LAN administrator from also having programming responsibilities.

NEW QUESTION 56

- (Topic 1)

Batch control reconciliation is a _____ (fill in the blank) control for mitigating risk of inadequate segregation of duties.

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

Answer: D

Explanation:

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

NEW QUESTION 59

- (Topic 1)

Key verification is one of the best controls for ensuring that:

- A. Data is entered correctly
- B. Only authorized cryptographic keys are used
- C. Input is authorized
- D. Database indexing is performed properly

Answer: A

Explanation:

Key verification is one of the best controls for ensuring that data is entered correctly.

NEW QUESTION 60

- (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 62

- (Topic 1)

What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?

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

Answer: B

Explanation:

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

NEW QUESTION 63

- (Topic 1)

How is the time required for transaction processing review usually affected by properly implemented Electronic Data Interface (EDI)?

- A. EDI usually decreases the time necessary for review

- B. EDI usually increases the time necessary for review
- C. Cannot be determined
- D. EDI does not affect the time necessary for review

Answer: A

Explanation:

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

NEW QUESTION 66

- (Topic 1)

What would an IS auditor expect to find in the console log? Choose the BEST answer.

- A. Evidence of password spoofing
- B. System errors
- C. Evidence of data copy activities
- D. Evidence of password sharing

Answer: B

Explanation:

An IS auditor can expect to find system errors to be detailed in the console log.

NEW QUESTION 67

- (Topic 1)

Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirety or not at all. Atomicity is part of the ACID test reference for transaction processing. True or false?

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 68

- (Topic 1)

What is the most common purpose of a virtual private network implementation?

- A. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such as the Internet
- B. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a dedicated T1 connection
- C. A virtual private network (VPN) helps to secure access within an enterprise when communicating over a dedicated T1 connection between network segments within the same facility
- D. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a wireless connection

Answer: A

Explanation:

A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such as the Internet.

NEW QUESTION 72

- (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 77

- (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 82

- (Topic 1)

Which of the following best characterizes "worms"?

- A. Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
- B. Programming code errors that cause a program to repeatedly dump data
- C. Malicious programs that require the aid of a carrier program such as email
- D. Malicious programs that masquerade as common applications such as screensavers or macro-enabled Word documents

Answer: A

Explanation:

Worms are malicious programs that can run independently and can propagate without the aid of a carrier program such as email.

NEW QUESTION 83

- (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 84

- (Topic 1)

How does the SSL network protocol provide confidentiality?

- A. Through symmetric encryption such as RSA
- B. Through asymmetric encryption such as Data Encryption Standard, or DES
- C. Through asymmetric encryption such as Advanced Encryption Standard, or AES
- D. Through symmetric encryption such as Data Encryption Standard, or DES

Answer: D

Explanation:

The SSL protocol provides confidentiality through symmetric encryption such as Data Encryption Standard, or DES.

NEW QUESTION 88

- (Topic 1)

Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

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

Answer: C

Explanation:

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

NEW QUESTION 93

- (Topic 1)

Which of the following is a good control for protecting confidential data residing on a PC?

- A. Personal firewall
- B. File encapsulation
- C. File encryption
- D. Host-based intrusion detection

Answer: C

Explanation:

File encryption is a good control for protecting confidential data residing on a PC.

NEW QUESTION 97

- (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 102

- (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 its own message digest from the data for comparison and data integrity validation
- 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 keys are used to enforce confidentiality. Hashing algorithms are used to enforce integrity.

NEW QUESTION 104

- (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 106

- (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 110

- (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 113

- (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 115

- (Topic 1)

Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

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

Answer: C

Explanation:

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

NEW QUESTION 120

- (Topic 1)

Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

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

Answer: A

Explanation:

A cold site is often an acceptable solution for preparing for recovery of noncritical systems and data.

NEW QUESTION 121

- (Topic 1)

Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the _____. (fill-in-the-blank)

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

Answer: C

Explanation:

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

NEW QUESTION 123

- (Topic 1)

Library control software restricts source code to:

- A. Read-only access
- B. Write-only access
- C. Full access
- D. Read-write access

Answer: A

Explanation:

Library control software restricts source code to read-only access.

NEW QUESTION 125

- (Topic 1)

When is regression testing used to determine whether new application changes have introduced any errors in the remaining unchanged code?

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

Answer: A

Explanation:

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

NEW QUESTION 127

- (Topic 1)

What is often the most difficult part of initial efforts in application development? Choose the BEST answer.

- A. Configuring software
- B. Planning security
- C. Determining time and resource requirements
- D. Configuring hardware

Answer: C

Explanation:

Determining time and resource requirements for an application-development project is often the most difficult part of initial efforts in application development.

NEW QUESTION 128

- (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 129

- (Topic 1)

What is a reliable technique for estimating the scope and cost of a software-development project?

- A. Function point analysis (FPA)
- B. Feature point analysis (FPA)
- C. GANTT
- D. PERT

Answer: A

Explanation:

A function point analysis (FPA) is a reliable technique for estimating the scope and cost of a software-development project.

NEW QUESTION 131

- (Topic 1)

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do? Choose the BEST answer.

- A. Lack of IT documentation is not usually material to the controls tested in an IT audi
- B. The auditor should at least document the informal standards and policie
- C. Furthermore, the IS auditor should create formal documented policies to be implemente
- D. The auditor should at least document the informal standards and policies, and test for complianc
- E. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemente
- F. The auditor should at least document the informal standards and policies, and test for complianc
- G. Furthermore, the IS auditor should create formal documented policies to be implemente

Answer: C

Explanation:

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, the auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented.

NEW QUESTION 136

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 140

- (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 144

- (Topic 1)

What can be used to help identify and investigate unauthorized transactions? Choose the BEST answer.

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

Answer: C

Explanation:

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

NEW QUESTION 148

- (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 152

- (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 156

- (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 161

- (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 162

- (Topic 1)

A check digit is an effective edit check to:

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

Answer: B

Explanation:

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

NEW QUESTION 167

- (Topic 1)

Parity bits are a control used to validate:

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

Answer: B

Explanation:

Parity bits are a control used to validate data completeness.

NEW QUESTION 172

- (Topic 1)

The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):

- A. Implementor
- B. Facilitator
- C. Developer
- D. Sponsor

Answer: B

Explanation:

The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a facilitator.

NEW QUESTION 176

- (Topic 1)

Which of the following is the MOST critical step in planning an audit?

- A. Implementing a prescribed auditing framework such as COBIT
- B. Identifying current controls
- C. Identifying high-risk audit targets
- D. Testing controls

Answer: C

Explanation:

In planning an audit, the most critical step is identifying the areas of high risk.

NEW QUESTION 180

- (Topic 1)

To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following? Choose the BEST answer.

- A. The business objectives of the organization
- B. The effect of segregation of duties on internal controls
- C. The point at which controls are exercised as data flows through the system
- D. Organizational control policies

Answer: C

Explanation:

When evaluating the collective effect of preventive, detective, or corrective controls within a process, an IS auditor should be aware of the point at which controls are exercised as data flows through the system.

NEW QUESTION 183

- (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 185

- (Topic 1)

Which of the following is of greatest concern to the IS auditor?

- A. Failure to report a successful attack on the network
- B. Failure to prevent a successful attack on the network
- C. Failure to recover from a successful attack on the network
- D. Failure to detect a successful attack on the network

Answer: A

Explanation:

Lack of reporting of a successful attack on the network is a great concern to an IS auditor.

NEW QUESTION 186

- (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 189

- (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 194

- (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 196

- (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 197

- (Topic 1)

Allowing application programmers to directly patch or change code in production programs increases risk of fraud. True or false?

- A. True
- B. False

Answer: A

Explanation:

Allowing application programmers to directly patch or change code in production programs increases risk of fraud.

NEW QUESTION 198

- (Topic 1)

Who should be responsible for network security operations?

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

Answer: B

Explanation:

Security administrators are usually responsible for network security operations.

NEW QUESTION 201

- (Topic 1)

Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 203

- (Topic 1)

What can be implemented to provide the highest level of protection from external attack?

- A. Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
- B. Configuring the firewall as a screened host behind a router
- C. Configuring the firewall as the protecting bastion host
- D. Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Answer: A

Explanation:

Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host provides a higher level of protection from external attack than all other answers.

NEW QUESTION 208

- (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 211

- (Topic 1)

How is the risk of improper file access affected upon implementing a database system?

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

Answer: D

Explanation:

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

NEW QUESTION 215

- (Topic 1)

In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

- A. The data should be deleted and overwritten with binary 0
- B. The data should be demagnetize
- C. The data should be low-level formatte
- D. The data should be delete

Answer: B

Explanation:

To properly protect against unauthorized disclosure of sensitive data, hard disks should be demagnetized before disposal or release.

NEW QUESTION 217

- (Topic 1)

When reviewing print systems spooling, an IS auditor is MOST concerned with which of the following vulnerabilities?

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

Answer: C

Explanation:

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

NEW QUESTION 222

- (Topic 1)

Why is the WAP gateway a component warranting critical concern and review for the IS auditor when auditing and testing controls enforcing message confidentiality?

- A. WAP is often configured by default settings and is thus insecur
- B. WAP provides weak encryption for wireless traffi
- C. WAP functions as a protocol-conversion gateway for wireless TLS to Internet SS
- D. WAP often interfaces critical IT system

Answer: C

Explanation:

Functioning as a protocol-conversion gateway for wireless TLS to Internet SSL, the WAP gateway is a component warranting critical concern and review for the IS auditor when auditing and testing controls that enforce message confidentiality.

NEW QUESTION 227

- (Topic 1)

Which of the following are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem? Choose the BEST answer.

- A. Expert systems
- B. Neural networks
- C. Integrated synchronized systems
- D. Multitasking applications

Answer: B

Explanation:

Neural networks are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem.

NEW QUESTION 231

- (Topic 1)

Which of the following can degrade network performance? Choose the BEST answer.

- A. Superfluous use of redundant load-sharing gateways
- B. Increasing traffic collisions due to host congestion by creating new collision domains
- C. Inefficient and superfluous use of network devices such as switches
- D. Inefficient and superfluous use of network devices such as hubs

Answer: D

Explanation:

Inefficient and superfluous use of network devices such as hubs can degrade network performance.

NEW QUESTION 233

- (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 236

- (Topic 1)

What is an effective control for granting temporary access to vendors and external support personnel? Choose the BEST answer.

- A. Creating user accounts that automatically expire by a predetermined date
- B. Creating permanent guest accounts for temporary use
- C. Creating user accounts that restrict logon access to certain hours of the day
- D. Creating a single shared vendor administrator account on the basis of least-privileged access

Answer: A

Explanation:

Creating user accounts that automatically expire by a predetermined date is an effective control for granting temporary access to vendors and external support personnel.

NEW QUESTION 241

- (Topic 1)

What is a common vulnerability, allowing denial-of-service attacks?

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

Answer: C

Explanation:

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

NEW QUESTION 244

- (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 248

- (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 249

- (Topic 1)

Which of the following fire-suppression methods is considered to be the most environmentally friendly?

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

Answer: C

Explanation:

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

NEW QUESTION 252

- (Topic 1)

What type of fire-suppression system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities?

- A. A dry-pipe sprinkler system
- B. A deluge sprinkler system
- C. A wet-pipe system
- D. A halon sprinkler system

Answer: A

Explanation:

A dry-pipe sprinkler system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities.

NEW QUESTION 257

- (Topic 1)

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

- A. False
- B. True

Answer: B

Explanation:

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

NEW QUESTION 260

- (Topic 1)

Which of the following provides the BEST single-factor authentication?

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

Answer: A

Explanation:

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

NEW QUESTION 263

- (Topic 1)

What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

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

Answer: C

Explanation:

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

NEW QUESTION 267

- (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 269

- (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 272

- (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 275

- (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 276

- (Topic 1)

When should systems administrators first assess the impact of applications or systems patches?

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

Answer: B

Explanation:

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

NEW QUESTION 281

- (Topic 1)

Organizations should use off-site storage facilities to maintain _____ (fill in the blank) of current and critical information within backup files. Choose the BEST answer.

- A. Confidentiality
- B. Integrity
- C. Redundancy
- D. Concurrency

Answer: C

Explanation:

Redundancy is the best answer because it provides both integrity and availability. Organizations should use off-site storage facilities to maintain redundancy of current and critical information within backup files.

NEW QUESTION 283

- (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 286

- (Topic 1)

What is an acceptable recovery mechanism for extremely time-sensitive transaction processing?

- A. Off-site remote journaling
- B. Electronic vaulting
- C. Shadow file processing
- D. Storage area network

Answer: C

Explanation:

Shadow file processing can be implemented as a recovery mechanism for extremely time-sensitive transaction processing.

NEW QUESTION 287

- (Topic 1)

Why is a clause for requiring source code escrow in an application vendor agreement important?

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

Answer: D

Explanation:

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

NEW QUESTION 292

- (Topic 1)

What uses questionnaires to lead the user through a series of choices to reach a conclusion? Choose the BEST answer.

- A. Logic trees
- B. Decision trees
- C. Decision algorithms
- D. Logic algorithms

Answer: B

Explanation:

Decision trees use questionnaires to lead the user through a series of choices to reach a conclusion.

NEW QUESTION 296

- (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 298

- (Topic 1)

An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to:

- A. Meet business objectives
- B. Enforce data security
- C. Be culturally feasible
- D. Be financially feasible

Answer: A

Explanation:

An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to meet business objectives.

NEW QUESTION 299

- (Topic 1)

Which of the following processes are performed during the design phase of the systemsdevelopment life cycle (SDLC) model?

- A. Develop test plan
- B. Baseline procedures to prevent scope creep
- C. Define the need that requires resolution, and map to the major requirements of the solution
- D. Program and test the new system
- E. The tests verify and validate what has been developed

Answer: B

Explanation:

Procedures to prevent scope creep are baselined in the design phase of the systems-development life cycle (SDLC) model.

NEW QUESTION 301

- (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 305

- (Topic 1)

What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality? Choose the BEST answer.

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

Answer: A

Explanation:

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

NEW QUESTION 307

- (Topic 1)

What kind of testing should programmers perform following any changes to an application or system?

- A. Unit, module, and full regression testing
- B. Module testing
- C. Unit testing
- D. Regression testing

Answer: A

Explanation:

Programmers should perform unit, module, and full regression testing following any changes to an application or system.

NEW QUESTION 308

- (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 313

- (Topic 1)

When should plans for testing for user acceptance be prepared? Choose the BEST answer.

- A. In the requirements definition phase of the systems-development project
- B. In the feasibility phase of the systems-development project
- C. In the design phase of the systems-development project
- D. In the development phase of the systems-development project

Answer: A

Explanation:

Plans for testing for user acceptance are usually prepared in the requirements definition phase of the systems-development project.

NEW QUESTION 316

- (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 319

- (Topic 1)

Input/output controls should be implemented for which applications in an integrated systems environment?

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

Answer: C

Explanation:

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

NEW QUESTION 322

- (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 323

- (Topic 1)

Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?

- A. Exposures
- B. Threats
- C. Hazards
- D. Insufficient controls

Answer: B

Explanation:

Threats exploit vulnerabilities to cause loss or damage to the organization and its assets.

NEW QUESTION 328

- (Topic 1)

Business process re-engineering often results in _____ automation, which results in _____ number of people using technology. Fill in the blanks.

- A. Increased; a greater
- B. Increased; a fewer
- C. Less; a fewer
- D. Increased; the same

Answer: A

Explanation:

Business process re-engineering often results in increased automation, which results in a greater number of people using technology.

NEW QUESTION 331

- (Topic 1)

Whenever business processes have been re-engineered, the IS auditor attempts to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes. True or false?

- A. True
- B. False

Answer: A

Explanation:

Whenever business processes have been re-engineered, the IS auditor should attempt to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes.

NEW QUESTION 336

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 341

- (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 344

- (Topic 1)

Data edits are implemented before processing and are considered which of the following? Choose the BEST answer.

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

Answer: D

Explanation:

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

NEW QUESTION 349

- (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 352

- (Topic 1)

What is a data validation edit control that matches input data to an occurrence rate? Choose the BEST answer.

- A. Accuracy check
- B. Completeness check
- C. Reasonableness check
- D. Redundancy check

Answer: C

Explanation:

A reasonableness check is a data validation edit control that matches input data to an occurrence rate.

NEW QUESTION 353

- (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 357

- (Topic 2)

The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

- A. Inherent
- B. Detection
- C. Control
- D. Business

Answer: B

Explanation:

Detection risks are directly affected by the auditor's selection of audit procedures and techniques. Inherent risks are not usually affected by an IS auditor. Control risks are controlled by the actions of the company's management. Business risks are not affected by an IS auditor.

NEW QUESTION 358

- (Topic 2)

Which of the following is a substantive test?

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

Answer: C

Explanation:

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

NEW QUESTION 360

- (Topic 2)

Which of the following is a benefit of a risk-based approach to audit planning? Audit:

- A. scheduling may be performed months in advance
- B. budgets are more likely to be met by the IS audit staff
- C. staff will be exposed to a variety of technologies
- D. resources are allocated to the areas of highest concern

Answer: D

Explanation:

The risk-based approach is designed to ensure audit time is spent on the areas of highest risk. The development of an audit schedule is not addressed by a risk-based approach. Audit schedules may be prepared months in advance using various scheduling methods. A risk approach does not have a direct correlation to the audit staff meeting time budgets on a particular audit, nor does it necessarily mean a wider variety of audits will be performed in a given year.

NEW QUESTION 363

- (Topic 2)

An audit charter should:

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

Answer: D

Explanation:

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

NEW QUESTION 364

- (Topic 2)

Which of the following sampling methods is MOST useful when testing for compliance?

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

Answer: A

Explanation:

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

NEW QUESTION 367

- (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 371

- (Topic 2)

An IS auditor is assigned to perform a postimplementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:

- A. implemented a specific control during the development of the application system
- B. designed an embedded audit module exclusively for auditing the application system
- C. participated as a member of the application system project team, but did not have operational responsibilities
- D. provided consulting advice concerning application system best practice

Answer: A

Explanation:

Independence may be impaired if an IS auditor is, or has been, actively involved in the development, acquisition and implementation of the application system. Choices B and C are situations that do not impair an IS auditor's independence. Choice D is incorrect because an IS auditor's independence is not impaired by providing advice on known best practices.

NEW QUESTION 375

- (Topic 2)

The PRIMARY advantage of a continuous audit approach is that it:

- A. does not require an IS auditor to collect evidence on system reliability while processing is taking place
- B. requires the IS auditor to review and follow up immediately on all information collected
- C. can improve system security when used in time-sharing environments that process a large number of transactions
- D. does not depend on the complexity of an organization's computer system

Answer: C

Explanation:

The use of continuous auditing techniques can improve system security when used in time-sharing environments that process a large number of transactions, but leave a scarce paper trail. Choice A is incorrect since the continuous audit approach often does require an IS auditor to collect evidence on system reliability while processing is taking place. Choice B is incorrect since an IS auditor normally would review and follow up only on material deficiencies or errors detected. Choice D is incorrect since the use of continuous audit techniques depends on the complexity of an organization's computer systems.

NEW QUESTION 379

- (Topic 2)

The PRIMARY purpose of audit trails is to:

- A. improve response time for user
- B. establish accountability and responsibility for processed transactions
- C. improve the operational efficiency of the system
- D. provide useful information to auditors who may wish to track transactions

Answer: B

Explanation:

Enabling audit trails helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system. The objective of enabling software to provide audit trails is not to improve system efficiency, since it often involves additional processing which may in fact reduce response time for users. Enabling audit trails involves storage and thus occupies disk space. Choice D is also a valid reason; however, it is not the primary reason.

NEW QUESTION 384

- (Topic 2)

When developing a risk-based audit strategy, an IS auditor should conduct a risk assessment to ensure that:

- A. controls needed to mitigate risks are in place
- B. vulnerabilities and threats are identified
- C. audit risks are considered
- D. a gap analysis is appropriate

Answer: B

Explanation:

In developing a risk-based audit strategy, it is critical that the risks and vulnerabilities be understood. This will determine the areas to be audited and the extent of

coverage. Understanding whether appropriate controls required to mitigate risks are in place is a resultant effect of an audit. Audit risks are inherent aspects of auditing, are directly related to the audit process and are not relevant to the risk analysis of the environment to be audited. A gap analysis would normally be done to compare the actual state to an expected or desirable state.

NEW QUESTION 386

- (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 388

- (Topic 2)

While planning an audit, an assessment of risk should be made to provide:

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

Answer: A

Explanation:

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

NEW QUESTION 393

- (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 398

- (Topic 2)

When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

- A. sufficient evidence will be collected
- B. all significant deficiencies identified will be corrected within a reasonable period
- C. all material weaknesses will be identified
- D. audit costs will be kept at a minimum level

Answer: A

Explanation:

Procedures are processes an IS auditor may follow in an audit engagement. In determining the appropriateness of any specific procedure, an IS auditor should use professional judgment appropriate to the specific circumstances. Professional judgment involves a subjective and often qualitative evaluation of conditions arising in the course of an audit. Judgment addresses a grey area where binary (yes/no) decisions are not appropriate and the auditor's past experience plays a key role in making a judgment. ISACA's guidelines provide information on how to meet the standards when performing IS audit work. Identifying material weaknesses is the result of appropriate competence, experience and thoroughness in planning and executing the audit and not of professional judgment. Professional judgment is not a primary input to the financial aspects of the audit.

NEW QUESTION 400

- (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 401

- (Topic 2)

An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

- A. Issue an audit finding
- B. Seek an explanation from IS management
- C. Review the classifications of data held on the server
- D. Expand the sample of logs reviewed

Answer: D

Explanation:

Audit standards require that an IS auditor gather sufficient and appropriate audit evidence. The auditor has found a potential problem and now needs to determine if this is an isolated incident or a systematic control failure. At this stage it is too preliminary to issue an audit finding and seeking an explanation from management is advisable, but it would be better to gather additional evidence to properly evaluate the seriousness of the situation. A backup failure, which has not been established at this point, will be serious if it involves critical data. However, the issue is not the importance of the data on the server, where a problem has been detected, but whether a systematic control failure that impacts other servers exists.

NEW QUESTION 402

- (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 407

- (Topic 2)

Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

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

Answer: A

Explanation:

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

NEW QUESTION 408

- (Topic 2)

During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

- A. create the procedures document

- B. terminate the audi
- C. conduct compliance testin
- D. identify and evaluate existing practice

Answer: D

Explanation:

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

NEW QUESTION 409

- (Topic 2)

In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

- A. identify and assess the risk assessment process used by managemen
- B. identify information assets and the underlying system
- C. disclose the threats and impacts to managemen
- D. identify and evaluate the existing control

Answer: D

Explanation:

It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

NEW QUESTION 413

- (Topic 2)

Which of the following should be of MOST concern to an IS auditor?

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

Answer: A

Explanation:

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

NEW QUESTION 414

- (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 419

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 424

- (Topic 2)

Which of the following would be the BEST population to take a sample from when testing program changes?

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

Answer: D

Explanation:

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

NEW QUESTION 425

- (Topic 2)

An integrated test facility is considered a useful audit tool because it:

- A. is a cost-efficient approach to auditing application control
- B. enables the financial and IS auditors to integrate their audit test
- C. compares processing output with independently calculated data
- D. provides the IS auditor with a tool to analyze a large range of information

Answer: C

Explanation:

An integrated test facility is considered a useful audit tool because it uses the same programs to compare processing using independently calculated data. This involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.

NEW QUESTION 429

- (Topic 2)

Data flow diagrams are used by IS auditors to:

- A. order data hierarchically
- B. highlight high-level data definition
- C. graphically summarize data paths and storage
- D. portray step-by-step details of data generation

Answer: C

Explanation:

Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of data. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

NEW QUESTION 430

- (Topic 2)

An IS auditor reviews an organizational chart PRIMARILY for:

- A. an understanding of workflow
- B. investigating various communication channels
- C. understanding the responsibilities and authority of individuals
- D. investigating the network connected to different employees

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 431

- (Topic 2)

An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

- A. Availability of online network documentation

- B. Support of terminal access to remote hosts
- C. Handling file transfer between hosts and interuser communications
- D. Performance management, audit and control

Answer: A

Explanation:

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

NEW QUESTION 433

- (Topic 2)

An IS auditor performing a review of an application's controls would evaluate the:

- A. efficiency of the application in meeting the business processe
- B. impact of any exposures discovere
- C. business processes served by the applicatio
- D. application's optimizatio

Answer: B

Explanation:

An application control review involves the evaluation of the application's automated controls and an assessment of any exposures resulting from the control weaknesses. The other choices may be objectives of an application audit but are not part of an audit restricted to a review of controls.

NEW QUESTION 438

- (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 443

- (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 444

- (Topic 2)

When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

- A. analysis
- B. evaluation
- C. preservation
- D. disclosure

Answer: C

Explanation:

Preservation and documentation of evidence for review by law enforcement and judicial authorities are of primary concern when conducting an investigation. Failure to properly preserve the evidence could jeopardize the acceptance of the evidence in legal proceedings. Analysis, evaluation and disclosure are important but not of primary concern in a forensic investigation.

NEW QUESTION 447

- (Topic 2)

The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

- A. confirm that the auditors did not overlook any important issue
- B. gain agreement on the finding
- C. receive feedback on the adequacy of the audit procedure
- D. test the structure of the final presentatio

Answer: B

Explanation:

The primary purpose for meeting with auditees prior to formally closing a review is to gain agreement on the findings. The other choices, though related to the formal closure of an audit, are of secondary importance.

NEW QUESTION 449

- (Topic 2)

The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

- A. comply with regulatory requirement
- B. provide a basis for drawing reasonable conclusion
- C. ensure complete audit coverag
- D. perform the audit according to the defined scop

Answer: B

Explanation:

The scope of an IS audit is defined by its objectives. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them. Complying with regulatory requirements, ensuring coverage and the execution of audit are all relevant to an audit but are not the reason why sufficient and relevant evidence is required.

NEW QUESTION 450

- (Topic 2)

After initial investigation, an IS auditor has reasons to believe that fraud may be present. The IS auditor should:

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

Answer: A

Explanation:

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

NEW QUESTION 454

- (Topic 2)

Which of the following would be the MOST effective audit technique for identifying segregation of duties violations in a new enterprise resource planning (ERP) implementation?

- A. Reviewing a report of security rights in the system
- B. Reviewing the complexities of authorization objects
- C. Building a program to identify conflicts in authorization
- D. Examining recent access rights violation cases

Answer: C

Explanation:

Since the objective is to identify violations in segregation of duties, it is necessary to define the logic that will identify conflicts in authorization. A program could be developed to identify these conflicts. A report of security rights in the enterprise resource planning (ERP) system would be voluminous and time consuming to review; therefore, this technique is not as effective as building a program. As complexities increase, it becomes more difficult to verify the effectiveness of the systems and complexity is not, in itself, a link to segregation of duties. It is good practice to review recent access rights violation cases; however, it may require a significant amount of time to truly identify which violations actually resulted from an inappropriate segregation of duties.

NEW QUESTION 456

- (Topic 2)

During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

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

Answer: C

Explanation:

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

NEW QUESTION 458

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

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 462

- (Topic 2)

An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

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

Answer: C

Explanation:

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

NEW QUESTION 466

- (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 470

- (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 474

- (Topic 2)

The final decision to include a material finding in an audit report should be made by the:

- A. audit committee
- B. auditee's management
- C. IS auditor
- D. CEO of the organization

Answer: C

Explanation:

The IS auditor should make the final decision about what to include or exclude from the audit report. The other choices would limit the independence of the auditor.

NEW QUESTION 477

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 480

- (Topic 2)

The success of control self-assessment (CSA) highly depends on:

- A. having line managers assume a portion of the responsibility for control monitoring
- B. assigning staff managers the responsibility for building, but not monitoring, controls
- C. the implementation of a stringent control policy and rule-driven controls
- D. the implementation of supervision and the monitoring of controls of assigned duties

Answer: A

Explanation:

The primary objective of a CSA program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional area line managers. The success of a control self-assessment (CSA) program depends on the degree to which line managers assume responsibility for controls. Choices B, C and D are characteristics of a traditional audit approach, not a CSA approach.

NEW QUESTION 485

- (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 486

- (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 assessment

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 490

- (Topic 3)

An IT steering committee should review information systems PRIMARILY to assess:

- A. whether IT processes support business requirement
- B. if proposed system functionality is adequate
- C. the stability of existing software
- D. the complexity of installed technology

Answer: A

Explanation:

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

NEW QUESTION 495

- (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 499

- (Topic 3)

IT governance is PRIMARILY the responsibility of the:

- A. chief executive office
- B. board of directors
- 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 503

- (Topic 3)

Effective IT governance requires organizational structures and processes to ensure that:

- A. the organization's strategies and objectives extend the IT strategy
- B. the business strategy is derived from an IT strategy
- C. IT governance is separate and distinct from the overall governance
- D. the IT strategy extends the organization's strategies and objectives

Answer: D

Explanation:

Effective IT governance requires that board and executive management extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives, and that the strategy is aligned with business strategy. Choice A is incorrect because it is the IT strategy that extends the organizational objectives, not the opposite. IT governance is not an isolated discipline; it must become an integral part of the overall enterprise governance.

NEW QUESTION 506

- (Topic 3)

The ultimate purpose of IT governance is to:

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

Answer: A

Explanation:

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

NEW QUESTION 511

- (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 516

- (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 competenc
- B. age, as training in audit techniques may be impractica
- C. IS knowledge, since this will bring enhanced credibility to the audit functio
- D. ability, as an IS auditor, to be independent of existing IS relationship

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 518

- (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 transferrates (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 522

- (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 526

- (Topic 3)

To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:

- A. enterprise data mode
- B. IT balanced scorecard (BSC).
- C. IT organizational structur
- D. historical financial statement

Answer: B

Explanation:

The IT balanced scorecard (BSC) is a tool that provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. An enterprise data model is a document defining the data structure of an organization and how data interrelate. It is useful, but it does not provide information on investments. The IT organizational structure provides an overview of the functional and reporting relationships in an IT entity. Historical financial statements do not provide information about planning and lack sufficient detail to enable one to fully understand management's activities regarding IT assets. Past costs do not necessarily reflect value, and assets such as data are not represented on the books of accounts.

NEW QUESTION 531

- (Topic 3)

Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?

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

Answer: B

Explanation:

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

NEW QUESTION 533

- (Topic 3)

To support an organization's goals, an IS department should have:

- A. a low-cost philosophy
- B. long- and short-range plan
- C. leading-edge technology
- D. plans to acquire new hardware and software

Answer: B

Explanation:

To ensure its contribution to the realization of an organization's overall goals, the IS department should have long- and short-range plans that are consistent with the organization's broader plans for attaining its goals. Choices A and C are objectives, and plans would be needed to delineate how each of the objectives would be achieved. Choice D could be a part of the overall plan but would be required only if hardware or software is needed to achieve the organizational goals.

NEW QUESTION 538

- (Topic 3)

Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?

- A. Allocating resources
- B. Keeping current with technology advances
- C. Conducting control self-assessment
- D. Evaluating hardware needs

Answer: A

Explanation:

The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department.

NEW QUESTION 539

- (Topic 3)

Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

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

Answer: D

Explanation:

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

NEW QUESTION 544

- (Topic 3)

An IS auditor reviewing an organization's IT strategic plan should FIRST review:

- A. the existing IT environment
- B. the business plan
- C. the present IT budget
- D. current technology trend

Answer: B

Explanation:

The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the business plan.

NEW QUESTION 546

.....

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