

Exam Questions CISA

Isaca CISA

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



NEW QUESTION 1

- (Topic 1)

Which of the following is a dynamic analysis tool for the purpose of testing software modules?

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

Answer: A

Explanation:

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

NEW QUESTION 2

- (Topic 1)

A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

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

Answer: A

Explanation:

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

NEW QUESTION 3

- (Topic 1)

To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:

- A. the entire message and thereafter enciphering the message digest using the sender's private ke
- B. any arbitrary part of the message and thereafter enciphering the message digest using the sender's private ke
- C. the entire message and thereafter enciphering the message using the sender's private ke
- D. the entire message and thereafter enciphering the message along with the message digest using the sender's private ke

Answer: A

Explanation:

A digital signature is a cryptographic method that ensures data integrity, authentication of the message, and non-repudiation. To ensure these, the sender first creates a message digest by applying a cryptographic hashing algorithm against the entire message and thereafter enciphers the message digest using the sender's private key. A message digest is created by applying a cryptographic hashing algorithm against the entire message not on any arbitrary part of the message. After creating the message digest, only the message digest is enciphered using the sender's private key, not the message.

NEW QUESTION 4

- (Topic 1)

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

- A. development and implementation of an information security standards manua
- B. performance of a comprehensive security control review by the IS audito
- C. adoption of a corporate information security policy statemen
- D. purchase of security access control softwar

Answer: C

Explanation:

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

NEW QUESTION 5

- (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 6

- (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 7

- (Topic 1)

What is the primary objective of a control self-assessment (CSA) program?

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

Answer: A

Explanation:

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

NEW QUESTION 8

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 9

- (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 10

- (Topic 1)

Who is accountable for maintaining appropriate security measures over information assets?

- A. Data and systems owners
- B. Data and systems users
- C. Data and systems custodians
- D. Data and systems auditors

Answer: A

Explanation:

Data and systems owners are accountable for maintaining appropriate security measures over information assets.

NEW QUESTION 10

- (Topic 1)

Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 11

- (Topic 1)

Who is ultimately accountable for the development of an IS security policy?

- A. The board of directors
- B. Middle management
- C. Security administrators
- D. Network administrators

Answer: A

Explanation:

The board of directors is ultimately accountable for the development of an IS security policy.

NEW QUESTION 12

- (Topic 1)

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

- A. Be inexpensive
- B. Be protected as sensitive confidential information
- C. Protect information confidentiality, integrity, and availability
- D. Support the business objectives of the organization

Answer: D

Explanation:

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

NEW QUESTION 15

- (Topic 1)

What topology provides the greatest redundancy of routes and the greatest network fault tolerance?

- A. A star network topology
- B. A mesh network topology with packet forwarding enabled at each host
- C. A bus network topology
- D. A ring network topology

Answer: B

Explanation:

A mesh network topology provides a point-to-point link between every network host. If each host is configured to route and forward communication, this topology provides the greatest redundancy of routes and the greatest network fault tolerance.

NEW QUESTION 18

- (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 20

- (Topic 1)

What can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program? Choose the BEST answer.

- A. Network-monitoring software
- B. A system downtime log
- C. Administration activity reports
- D. Help-desk utilization trend reports

Answer: B

Explanation:

A system downtime log can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program.

NEW QUESTION 25

- (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 28

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 29

- (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 33

- (Topic 1)

What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?

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

Answer: C

Explanation:

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

NEW QUESTION 35

- (Topic 1)

Regarding digital signature implementation, which of the following answers is correct?

- A. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's private ke
- B. Upon receiving the data, the recipient can decrypt the data using the sender's public ke
- C. A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public ke
- D. Upon receiving the data, the recipient can decrypt the data using the recipient's public ke

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

Answer: C

Explanation:

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

NEW QUESTION 37

- (Topic 1)

Which of the following would provide the highest degree of server access control?

- A. A mantrap-monitored entryway to the server room
- B. Host-based intrusion detection combined with CCTV
- C. Network-based intrusion detection
- D. A fingerprint scanner facilitating biometric access control

Answer: D

Explanation:

A fingerprint scanner facilitating biometric access control can provide a very high degree of server access control.

NEW QUESTION 38

- (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 39

- (Topic 1)

What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off? Choose the BEST answer.

- A. Employee security awareness training
- B. Administrator alerts
- C. Screensaver passwords
- D. Close supervision

Answer: C

Explanation:

Screensaver passwords are an effective control to implement as a countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off.

NEW QUESTION 43

- (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 44

- (Topic 1)

What is the key distinction between encryption and hashing algorithms?

- A. Hashing algorithms ensure data confidentialit

- 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 49

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 53

- (Topic 1)

What type of BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness?

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

Answer: B

Explanation:

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

NEW QUESTION 54

- (Topic 1)

Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

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

Answer: A

Explanation:

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

NEW QUESTION 59

- (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 60

- (Topic 1)

Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

- A. True

B. False

Answer: A

Explanation:

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

NEW QUESTION 63

- (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 67

- (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 70

- (Topic 1)

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

- A. True
- B. False

Answer: B

Explanation:

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

NEW QUESTION 73

- (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 75

- (Topic 1)

What often results in project scope creep when functional requirements are not defined as well as they could be?

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

Answer: A

Explanation:

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

NEW QUESTION 80

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 83

- (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 85

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 89

- (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 94

- (Topic 1)

A transaction journal provides the information necessary for detecting unauthorized _____ (fill in the blank) from a terminal.

- A. Deletion
- B. Input
- C. Access
- D. Duplication

Answer: B

Explanation:

A transaction journal provides the information necessary for detecting unauthorized input from a terminal.

NEW QUESTION 95

- (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 99

- (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 100

- (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 compensator 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 102

- (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 107

- (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 112

- (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 114

- (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 116

- (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 120

- (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 123

- (Topic 1)

What supports data transmission through split cable facilities or duplicate cable facilities?

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

Answer: A

Explanation:

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

NEW QUESTION 128

- (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 131

- (Topic 1)

Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

- A. Traffic analysis
- B. SYN flood
- C. Denial of service (DoS)
- D. Distributed denial of service (DoS)

Answer: A

Explanation:

Traffic analysis is a passive attack method used by intruders to determine potential network vulnerabilities. All others are active attacks.

NEW QUESTION 136

- (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 137

- (Topic 1)

Which of the following is of greatest concern when performing an IS audit?

- A. Users' ability to directly modify the database
- B. Users' ability to submit queries to the database
- C. Users' ability to indirectly modify the database
- D. Users' ability to directly view the database

Answer: A

Explanation:

A major IS audit concern is users' ability to directly modify the database.

NEW QUESTION 138

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 140

- (Topic 1)

Off-site data backup and storage should be geographically separated so as to _____ (fill in the blank) the risk of a widespread physical disaster such as a hurricane or earthquake.

- A. Accept
- B. Eliminate
- C. Transfer
- D. Mitigate

Answer: D

Explanation:

Off-site data backup and storage should be geographically separated, to mitigate the risk of a widespread physical disaster such as a hurricane or an earthquake.

NEW QUESTION 145

- (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 148

- (Topic 1)

Test and development environments should be separated. True or false?

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 150

- (Topic 1)

What is the most common reason for information systems to fail to meet the needs of users? Choose the BEST answer.

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

Answer: B

Explanation:

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

NEW QUESTION 152

- (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 153

- (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 154

- (Topic 1)

Authentication techniques for sending and receiving data between EDI systems is crucial to prevent which of the following? Choose the BEST answer.

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

Answer: B

Explanation:

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

NEW QUESTION 155

- (Topic 1)

What is the primary security concern for EDI environments? Choose the BEST answer.

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

Answer: D

Explanation:

Transaction authorization is the primary security concern for EDI environments.

NEW QUESTION 156

- (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 160

- (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 163

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 165

- (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 170

- (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 172

- (Topic 2)

The PRIMARY purpose of audit trails is to:

- A. improve response time for user
- B. establish accountability and responsibility for processed transaction
- 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 173

- (Topic 2)

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

- A. address audit objective
- B. collect sufficient evidence
- C. specify appropriate test
- D. minimize audit resource

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 177

- (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 180

- (Topic 2)

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

- A. CASE tools
- B. Embedded data collection tools
- C. Heuristic scanning tools
- D. Trend/variance detection tools

Answer: D

Explanation:

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

NEW QUESTION 181

- (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 186

CORRECT TEXT - (Topic 2)

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

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

Answer: B

NEW QUESTION 189

- (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 191

- (Topic 2)

Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

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

Answer: C

Explanation:

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

NEW QUESTION 196

- (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 199

- (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 200

- (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 203

- (Topic 2)

An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

- A. conclude that the controls are inadequate
- B. expand the scope to include substantive testing
- C. place greater reliance on previous audit
- D. suspend the audit

Answer: B

Explanation:

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

NEW QUESTION 204

- (Topic 2)

Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

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

Answer: B

Explanation:

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

NEW QUESTION 205

- (Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 207

- (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 208

- (Topic 2)

Which of the following would an IS auditor use to determine if unauthorized modifications were made to production programs?

- A. System log analysis
- B. Compliance testing
- C. Forensic analysis
- D. Analytical review

Answer: B

Explanation:

Determining that only authorized modifications are made to production programs would require the change management process be reviewed to evaluate the existence of a trail of documentary evidence. Compliance testing would help to verify that the change management process has been applied consistently. It is unlikely that the system log analysis would provide information about the modification of programs. Forensic analysis is a specialized technique for criminal investigation. An analytical review assesses the general control environment of an organization.

NEW QUESTION 209

- (Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 212

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 216

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 218

- (Topic 2)

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

- A. statements from IS management
- B. workpapers of other auditors
- C. an organizational control self-assessment
- D. sufficient and appropriate audit evidence

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 219

- (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 risks
- C. can be used as a replacement for traditional audit
- D. allows management to relinquish responsibility for control

Answer: A

Explanation:

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

NEW QUESTION 220

- (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, control
- C. the implementation of a stringent control policy and rule-driven control

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 222

- (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 224

- (Topic 3)

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

- A. whether IT processes support business requirements
- 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 225

- (Topic 3)

As an outcome of information security governance, strategic alignment provides:

- A. security requirements driven by enterprise requirements
- B. baseline security following best practice
- C. institutionalized and commoditized solutions
- D. an understanding of risk exposure

Answer: A

Explanation:

Information security governance, when properly implemented, should provide four basic outcomes: strategic alignment, value delivery, risk management and performance measurement. Strategic alignment provides input for security requirements driven by enterprise requirements. Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. Risk management provides an understanding of risk exposure.

NEW QUESTION 229

- (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 232

- (Topic 3)

Which of the following is the MOST important element for the successful implementation of IT governance?

- A. Implementing an IT scorecard
- B. Identifying organizational strategies
- C. Performing a risk assessment
- D. Creating a formal security policy

Answer: B

Explanation:

The key objective of an IT governance program is to support the business, thus the identification of organizational strategies is necessary to ensure alignment between IT and corporate governance. Without identification of organizational strategies, the remaining choices—even if implemented—would be ineffective.

NEW QUESTION 233

- (Topic 3)

The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

- A. IT budget
- B. existing IT environment
- C. business plan
- D. investment plan

Answer: C

Explanation:

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

NEW QUESTION 234

- (Topic 3)

The ultimate purpose of IT governance is to:

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

Answer: A

Explanation:

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

NEW QUESTION 238

- (Topic 3)

Responsibility for the governance of IT should rest with the:

- A. IT strategy committee
- B. chief information officer (CIO)
- C. audit committee
- D. board of directors

Answer: D

Explanation:

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

NEW QUESTION 239

- (Topic 3)

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

- A. ensure the employee maintains a good quality of life, which will lead to greater productivity
- B. reduce the opportunity for an employee to commit an improper or illegal act
- C. provide proper cross-training for another employee

D. eliminate the potential disruption caused when an employee takes vacation one day at a time

Answer: B

Explanation:

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

NEW QUESTION 241

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 244

- (Topic 3)

When segregation of duties concerns exist between IT support staff and end users, what would be a suitable compensating control?

- A. Restricting physical access to computing equipment
- B. Reviewing transaction and application logs
- C. Performing background checks prior to hiring IT staff
- D. Locking user sessions after a specified period of inactivity

Answer: B

Explanation:

Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure IT staff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently) of access privileges that have officially been granted.

NEW QUESTION 245

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 247

- (Topic 3)

Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

- A. Deleting database activity logs
- B. Implementing database optimization tools
- C. Monitoring database usage
- D. Defining backup and recovery procedures

Answer: A

Explanation:

Since database activity logs record activities performed by the database administrator (DBA), deleting them should be performed by an individual other than the DBA. This is a compensating control to aid in ensuring an appropriate segregation of duties and is associated with the DBA's role. A DBA should perform the other activities as part of the normal operations.

NEW QUESTION 251

- (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 255

- (Topic 3)

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

- A. a low-cost philosoph
- B. long- and short-range plan
- C. leading-edge technolog
- D. plans to acquire new hardware and softwar

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 258

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 261

- (Topic 3)

When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

- A. has all the personnel and equipment it need
- B. plans are consistent with management strateg
- C. uses its equipment and personnel efficiently and effective
- D. has sufficient excess capacity to respond to changing direction

Answer: B

Explanation:

Determining if the IS plan is consistent with management strategy relates IS/IT planning to business plans. Choices A, C and D are effective methods for determining the alignment of IS plans with business objectives and the organization's strategies.

NEW QUESTION 265

- (Topic 3)

A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

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

Answer: B

Explanation:

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

NEW QUESTION 267

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 269

- (Topic 3)

When developing a security architecture, which of the following steps should be executed FIRST?

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

Answer: B

Explanation:

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

NEW QUESTION 273

- (Topic 3)

An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

- A. report that the control is operating effectively since deactivation happens within the time frame stated in the IS polic
- B. verify that user access rights have been granted on a need-to-have basi
- C. recommend changes to the IS policy to ensure deactivation of user IDs upon terminatio
- D. recommend that activity logs of terminated users be reviewed on a regular basi

Answer: C

Explanation:

Although a policy provides a reference for performing IS audit assignments, an IS auditor needs to review the adequacy and the appropriateness of the policy. If, in the opinion of the auditor, the time frame defined for deactivation is inappropriate, the auditor needs to communicate this to management and recommend changes to the policy. Though the deactivation happens as stated in the policy, it cannot be concluded that the control is effective. Best practice would require that the ID of a terminated user be deactivated immediately. Verifying that user access rights have been granted on a need-to-have basis is necessary when permissions are granted. Recommending that activity logs of terminated users be reviewed on a regular basis is a good practice, but not as effective as deactivation upon termination.

NEW QUESTION 278

- (Topic 3)

An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should FIRST verify that the:

- A. technical platforms between the two companies are interoperabl
- B. parent bank is authorized to serve as a service provide

- C. security features are in place to segregate subsidiary trade
- D. subsidiary can join as a co-owner of this payment system

Answer: B

Explanation:

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

NEW QUESTION 282

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 286

- (Topic 3)

When an organization is outsourcing their information security function, which of the following should be kept in the organization?

- A. Accountability for the corporate security policy
- B. Defining the corporate security policy
- C. Implementing the corporate security policy
- D. Defining security procedures and guidelines

Answer: A

Explanation:

Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

NEW QUESTION 290

- (Topic 3)

An organization has outsourced its help desk activities. An IS auditor's GREATEST concern when reviewing the contract and associated service level agreement (SLA) between the organization and vendor should be the provisions for:

- A. documentation of staff background check
- B. independent audit reports or full audit access
- C. reporting the year-to-year incremental cost reduction
- D. reporting staff turnover, development or training

Answer: B

Explanation:

When the functions of an IS department are outsourced, an IS auditor should ensure that a provision is made for independent audit reports that cover all essential areas, or that the outsourcer has full audit access. Although it is necessary to document the fact that background checks are performed, this is not as important as provisions for audits. Financial measures such as year-to-year incremental cost reductions are desirable to have in a service level agreement (SLA); however, cost reductions are not as important as the availability of independent audit reports or full audit access. An SLA might include human relationship measures such as resource planning, staff turnover, development or training, but this is not as important as the requirements for independent reports or full audit access by the outsourcing organization.

NEW QUESTION 293

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 296

- (Topic 3)

Assessing IT risks is BEST achieved by:

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

Answer: A

Explanation:

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

NEW QUESTION 298

- (Topic 3)

To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

- A. avoidance
- B. transference
- C. mitigation
- D. acceptance

Answer: C

Explanation:

Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.

NEW QUESTION 300

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 303

- (Topic 3)

As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

- A. performance measurement
- B. strategic alignment
- C. value delivery
- D. resource management

Answer: A

Explanation:

Performance measurement includes setting and monitoring measurable objectives of what the IT processes need to deliver (process outcome) and how they deliver it (process capability and performance). Strategic alignment primarily focuses on ensuring linkage of business and IT plans. Value delivery is about executing the value proposition throughout the delivery cycle. Resource management is about the optimal investment in and proper management of critical IT resources. Transparency is primarily achieved through performance measurement as it provides information to the stakeholders on how well the enterprise is performing when compared to objectives.

NEW QUESTION 305

- (Topic 3)

Before implementing an IT balanced scorecard, an organization must:

- A. deliver effective and efficient service
- B. define key performance indicator
- C. provide business value to IT project
- D. control IT expense

Answer: B

Explanation:

A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

NEW QUESTION 310

- (Topic 3)

Which of the following is the PRIMARY objective of an IT performance measurement process?

- A. Minimize errors
- B. Gather performance data
- C. Establish performance baselines
- D. Optimize performance

Answer: D

Explanation:

An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of IT measurement process and would be used to evaluate the performance against previously established performance baselines.

NEW QUESTION 312

- (Topic 4)

When auditing the proposed acquisition of a new computer system, an IS auditor should FIRST establish that:

- A. a clear business case has been approved by management
- B. corporate security standards will be met
- C. users will be involved in the implementation plan
- D. the new system will meet all required user functionalities

Answer: A

Explanation:

The first concern of an IS auditor should be to establish that the proposal meets the needs of the business, and this should be established by a clear business case. Although compliance with security standards is essential, as is meeting the needs of the users and having users involved in the implementation process, it is too early in the procurement process for these to be an IS auditor's first concern.

NEW QUESTION 315

- (Topic 4)

Change control for business application systems being developed using prototyping could be complicated by the:

- A. iterative nature of prototyping
- B. rapid pace of modifications in requirements and design
- C. emphasis on reports and screens
- D. lack of integrated tool

Answer: B

Explanation:

Changes in requirements and design happen so quickly that they are seldom documented or approved. Choices A, C and D are characteristics of prototyping, but they do not have an adverse effect on change control.

NEW QUESTION 319

- (Topic 4)

An IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could an IS auditor use to estimate the size of the development effort?

- A. Program evaluation review technique (PERT)
- B. Counting source lines of code (SLOC)
- C. Function point analysis
- D. White box testing

Answer: C

Explanation:

Function point analysis is an indirect method of measuring the size of an application by considering the number and complexity of its inputs, outputs and files. It is useful for evaluating complex applications. PERT is a project management technique that helps with both planning and control. SLOC gives a direct measure of program size, but does not allow for the complexity that may be caused by having multiple, linked modules and a variety of inputs and outputs. White box testing involves a detailed review of the behavior of program code, and is a quality assurance technique suited to simpler applications during the design and build stage of development.

NEW QUESTION 324

- (Topic 4)

When planning to add personnel to tasks imposing time constraints on the duration of a project, which of the following should be revalidated FIRST?

- A. The project budget
- B. The critical path for the project
- C. The length of the remaining tasks
- D. The personnel assigned to other tasks

Answer: B

Explanation:

Since adding resources may change the route of the critical path, the critical path must be reevaluated to ensure that additional resources will in fact shorten the project duration. Given that there may be slack time available on some of the other tasks not on the critical path, factors such as the project budget, the length of other tasks and the personnel assigned to them may or may not be affected.

NEW QUESTION 327

- (Topic 4)

Which of the following is a characteristic of timebox management?

- A. Not suitable for prototyping or rapid application development (RAD)
- B. Eliminates the need for a quality process
- C. Prevents cost overruns and delivery delays
- D. Separates system and user acceptance testing

Answer: C

Explanation:

Timebox management, by its nature, sets specific time and cost boundaries. It is very suitable for prototyping and RAD, and integrates system and user acceptance testing, but does not eliminate the need for a quality process.

NEW QUESTION 332

- (Topic 4)

Which of the following should an IS auditor review to gain an understanding of the effectiveness of controls over the management of multiple projects?

- A. Project database
- B. Policy documents
- C. Project portfolio database
- D. Program organization

Answer: C

Explanation:

A project portfolio database is the basis for project portfolio management. It includes project data, such as owner, schedules, objectives, project type, status and cost. Project portfolio management requires specific project portfolio reports. A project database may contain the above for one specific project and updates to various parameters pertaining to the current status of that single project. Policy documents on project management set direction for the design, development, implementation and monitoring of the project. Program organization is the team required (steering committee, quality assurance, systems personnel, analyst, programmer, hardware support, etc.) to meet the delivery objective of the project.

NEW QUESTION 335

- (Topic 4)

While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

- A. effectiveness of the QA function because it should interact between project management and user management
- B. efficiency of the QA function because it should interact with the project implementation team
- C. effectiveness of the project manager because the project manager should interact with the QA function
- D. efficiency of the project manager because the QA function will need to communicate with the project implementation team

Answer: A

Explanation:

To be effective the quality assurance (QA) function should be independent of project management. The QA function should never interact with the project implementation team since this can impact effectiveness. The project manager does not interact with the QA function, which should not impact the effectiveness of the project manager. The QA function does not interact with the project implementation team, which should not impact the efficiency of the project manager.

NEW QUESTION 339

- (Topic 4)

When reviewing a project where quality is a major concern, an IS auditor should use the project management triangle to explain that:

- A. increases in quality can be achieved, even if resource allocation is decrease
- B. increases in quality are only achieved if resource allocation is increase
- C. decreases in delivery time can be achieved, even if resource allocation is decrease
- D. decreases in delivery time can only be achieved if quality is decrease

Answer: A

Explanation:

The three primary dimensions of a project are determined by the deliverables, the allocated resources and the delivery time. The area of the project management triangle, comprised of these three dimensions, is fixed. Depending on the degree of freedom, changes in one dimension might be compensated by changing either one or both remaining dimensions. Thus, if resource allocation is decreased an increase in quality can be achieved, if a delay in the delivery time of the project will be accepted. The area of the triangle always remains constant.

NEW QUESTION 340

- (Topic 4)

A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

- A. IS auditor
- B. Database administrator
- C. Project manager
- D. Data owner

Answer: D

Explanation:

During the data conversion stage of a project, the data owner is primarily responsible for reviewing and signing-off that the data are migrated completely, accurately and are valid. An IS auditor is not responsible for reviewing and signing-off on the accuracy of the converted data. However, an IS auditor should ensure that there is a review and sign-off by the data owner during the data conversion stage of the project. A database administrator's primary responsibility is to maintain the integrity of the database and make the database available to users. A database administrator is not responsible for reviewing migrated data. A project manager provides day-to-day management and leadership of the project, but is not responsible for the accuracy and integrity of the data.

NEW QUESTION 343

- (Topic 4)

A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

- A. what amount of progress against schedule has been achieved
- B. if the project budget can be reduced
- C. if the project could be brought in ahead of schedule
- D. if the budget savings can be applied to increase the project scope

Answer: A

Explanation:

Cost performance of a project cannot be properly assessed in isolation of schedule performance. Cost cannot be assessed simply in terms of elapsed time on a project. To properly assess the project budget position it is necessary to know how much progress has actually been made and, given this, what level of expenditure would be expected. It is possible that project expenditure appears to be low because actual progress has been slow. Until the analysis of project against schedule has been completed, it is impossible to know whether there is any reason to reduce budget, if the project has slipped behind schedule, then not only may there be no spare budget but it is possible that extra expenditure may be needed to retrieve the slippage. The low expenditure could actually be representative of a situation where the project is likely to miss deadlines rather than potentially come in ahead of time. If the project is found to be ahead of budget after adjusting for actual progress, this is not necessarily a good outcome because it points to flaws in the original budgeting process; and, as said above, until further analysis is undertaken, it cannot be determined whether any spare funds actually exist. Further, if the project is behind schedule, then adding scope may be the wrong thing to do.

NEW QUESTION 344

- (Topic 4)

A manager of a project was not able to implement all audit recommendations by the target date. The IS auditor should:

- A. recommend that the project be halted until the issues are resolved
- B. recommend that compensating controls be implemented
- C. evaluate risks associated with the unresolved issue
- D. recommend that the project manager reallocate test resources to resolve the issue

Answer: C

Explanation:

It is important to evaluate what the exposure would be when audit recommendations have not been completed by the target date. Based on the evaluation, management can accordingly consider compensating controls, risk acceptance, etc. All other choices might be appropriate only after the risks have been assessed.

NEW QUESTION 345

- (Topic 4)

The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

- A. integrit
- B. authenticit
- C. authorizatio
- D. nonrepudiatio

Answer: A

Explanation:

A checksum calculated on an amount field and included in the EDI communication can be used to identify unauthorized modifications. Authenticity and authorization cannot be established by a checksum alone and need other controls. Nonrepudiation can be ensured by using digital signatures.

NEW QUESTION 347

- (Topic 4)

Before implementing controls, management should FIRST ensure that the controls:

- A. satisfy a requirement in addressing a risk issu
- B. do not reduce productivit
- C. are based on a cost-benefit analysi
- D. are detective or correctiv

Answer: A

Explanation:

When designing controls, it is necessary to consider all the above aspects. In an ideal situation, controls that address all these aspects would be the best controls. Realistically, it may not be possible to design them all and cost may be prohibitive; therefore, it is necessary to first consider the preventive controls that attack the cause of a threat.

NEW QUESTION 350

- (Topic 4)

Information for detecting unauthorized input from a terminal would be BEST provided by the:

- A. console log printou
- B. transaction journa
- C. automated suspense file listin
- D. user error repor

Answer: B

Explanation:

The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error occurred, while the user error report would only list input that resulted in an edit error.

NEW QUESTION 355

- (Topic 4)

Functional acknowledgements are used:

- A. as an audit trail for EDI transaction
- B. to functionally describe the IS departmen
- C. to document user roles and responsibilitie
- D. as a functional description of application softwar

Answer: A

Explanation:

Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

NEW QUESTION 358

- (Topic 4)

A proposed transaction processing application will have many data capture sources and outputs in paper and electronic form. To ensure that transactions are not lost during processing, an IS auditor should recommend the inclusion of:

- A. validation control
- B. internal credibility check
- C. clerical control procedure
- D. automated systems balancin

Answer:

D

Explanation:

Automated systems balancing would be the best way to ensure that no transactions are lost as any imbalance between total inputs and total outputs would be reported for investigation and correction. Validation controls and internal credibility checks are certainly valid controls, but will not detect and report lost transactions. In addition, although a clerical procedure could be used to summarize and compare inputs and outputs, an automated process is less susceptible to error.

NEW QUESTION 363

- (Topic 4)

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, e.g., an incorrect, but valid, value substituted for the original. This control is effective in detecting transposition and transcription errors. A range check is checking data that matches a predetermined range of values. A validity check is programmed checking of the data validity in accordance with predetermined criteria. In a duplicate check, new or fresh transactions are matched to those previously entered to ensure that they are not already in the system.

NEW QUESTION 365

- (Topic 4)

A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

- A. Establishing an inter-networked system of client servers with suppliers for increased efficiencies
- B. Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing
- C. Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format
- D. Reengineering the existing processing and redesigning the existing system

Answer: C**Explanation:**

EDI is the best answer. Properly implemented (e.g., agreements with trading partners transaction standards, controls over network security mechanisms in conjunction with application controls), EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

NEW QUESTION 366

- (Topic 4)

An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

- A. continuous improvement
- B. quantitative quality goal
- C. a documented process
- D. a process tailored to specific project

Answer: A**Explanation:**

An organization would have reached the highest level of the software CMM at level 5, optimizing. Quantitative quality goals can be reached at level 4 and below, a documented process is executed at level 3 and below, and a process tailored to specific projects can be achieved at level 3 or below.

NEW QUESTION 371

- (Topic 4)

Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?

- A. inheritance
- B. Dynamic warehousing
- C. Encapsulation
- D. Polymorphism

Answer: C**Explanation:**

Encapsulation is a property of objects, and it prevents accessing either properties or methods that have not been previously defined as public. This means that any implementation of the behavior of an object is not accessible. An object defines a communication interface with the exterior and only that which belongs to that interface can be accessed.

NEW QUESTION 372

- (Topic 4)

The phases and deliverables of a system development life cycle (SDLC) project should be determined:

- A. during the initial planning stages of the project
- B. after early planning has been completed, but before work has begun
- C. throughout the work stages, based on risks and exposure
- D. only after all risks and exposures have been identified and the IS auditor has recommended appropriate control

Answer: A

Explanation:

It is extremely important that the project be planned properly and that the specific phases and deliverables be identified during the early stages of the project.

NEW QUESTION 375

- (Topic 4)

When implementing an application software package, which of the following presents the GREATEST risk?

- A. Uncontrolled multiple software versions
- B. Source programs that are not synchronized with object code
- C. incorrectly set parameters
- D. Programming error

Answer: C

Explanation:

Parameters that are not set correctly would be the greatest concern when implementing an application software package. The other choices, though important, are a concern of the provider, not the organization that is implementing the software itself.

NEW QUESTION 376

CORRECT TEXT - (Topic 4)

Which of the following is an advantage of prototyping?

- A. The finished system normally has strong internal control
- B. Prototype systems can provide significant time and cost saving
- C. Change control is often less complicated with prototype system
- D. it ensures that functions or extras are not added to the intended system

Answer: B

NEW QUESTION 380

- (Topic 4)

An advantage of using sanitized live transactions in test data is that:

- A. all transaction types will be included
- B. every error condition is likely to be tested
- C. no special routines are required to assess the result
- D. test transactions are representative of live processing

Answer: D

Explanation:

Test data will be representative of live processing; however, it is unlikely that all transaction types or error conditions will be tested in this way.

NEW QUESTION 382

- (Topic 4)

Which of the following should be included in a feasibility study for a project to implement an EDI process?

- A. The encryption algorithm format
- B. The detailed internal control procedures
- C. The necessary communication protocols
- D. The proposed trusted third-party agreement

Answer: C

Explanation:

Encryption algorithms, third-party agreements and internal control procedures are too detailed for this phase. They would only be outlined and any cost or performance implications shown. The communications protocols must be included, as there may be significant cost implications if new hardware and software are involved, and risk implications if the technology is new to the organization.

NEW QUESTION 386

- (Topic 4)

During the development of an application, the quality assurance testing and user acceptance testing were combined. The MAJOR concern for an IS auditor

reviewing the project is that there will be:

- A. increased maintenanc
- B. improper documentation of testin
- C. inadequate functional testin
- D. delays in problem resolutio

Answer: C

Explanation:

The major risk of combining quality assurance testing and user acceptance testing is that functional testing may be inadequate. Choices A, B and D are not as important.

NEW QUESTION 391

- (Topic 4)

The GREATEST advantage of rapid application development (RAD) over the traditional system development life cycle (SDLC) is that it:

- A. facilitates user involvemen
- B. allows early testing of technical feature
- C. facilitates conversion to the new syste
- D. shortens the development time fram

Answer: D

Explanation:

The greatest advantage of RAD is the shorter time frame for the development of a system. Choices A and B are true, but they are also true for the traditional systems development life cycle. Choice C is not necessarily always true.

NEW QUESTION 395

- (Topic 4)

By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:

- A. reliable products are guarantee
- B. programmers' efficiency is improve
- C. security requirements are designe
- D. predictable software processes are followe

Answer: D

Explanation:

By evaluating the organization's development projects against the CMM, an IS auditor determines whether the development organization follows a stable, predictable software process. Although the likelihood of success should increase as the software processes mature toward the optimizing level, mature processes do not guarantee a reliable product. CMM does not evaluate technical processes such as programming nor does it evaluate security requirements or other application controls.

NEW QUESTION 396

- (Topic 4)

Which testing approach is MOST appropriate to ensure that internal application interface errors are identified as soon as possible?

- A. Bottom up
- B. Sociability testing
- C. Top-down
- D. System test

Answer: C

Explanation:

The top-down approach to testing ensures that interface errors are detected early and that testing of major functions is conducted early. A bottom-up approach to testing begins with atomic units, such as programs and modules, and works upward until a complete system test has taken place. Sociability testing and system tests take place at a later stage in the development process.

NEW QUESTION 399

- (Topic 4)

During the system testing phase of an application development project the IS auditor should review the:

- A. conceptual design specification
- B. vendor contrac
- C. error report
- D. program change request

Answer: C

Explanation:

Testing is crucial in determining that user requirements have been validated. The IS auditor should be involved in this phase and review error reports for their precision in recognizing erroneous data and review the procedures for resolving errors. A conceptual design specification is a document prepared during the requirements definition phase. A vendor contract is prepared during a software acquisition process. Program change requests would normally be reviewed as a part of the postimplementation phase.

NEW QUESTION 403

- (Topic 4)

Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?

- A. increase the time allocated for system testing
- B. implement formal software inspections
- C. increase the development staff
- D. Require the sign-off of all project deliverables

Answer: B

Explanation:

Inspections of code and design are a proven software quality technique. An advantage of this approach is that defects are identified before they propagate through the development life cycle. This reduces the cost of correction as less rework is involved. Allowing more time for testing may discover more defects; however, little is revealed as to why the quality problems are occurring and the cost of the extra testing, and the cost of rectifying the defects found will be greater than if they had been discovered earlier in the development process. The ability of the development staff can have a bearing on the quality of what is produced; however, replacing staff can be expensive and disruptive, and the presence of a competent staff cannot guarantee quality in the absence of effective quality management processes. Sign-off of deliverables may help detect defects if signatories are diligent about reviewing deliverable content; however, this is difficult to enforce. Deliverable reviews normally do not go down to the same level of detail as software inspections.

NEW QUESTION 406

- (Topic 4)

Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

- A. System owners
- B. System users
- C. System designers
- D. System builders

Answer: A

Explanation:

System owners are the information systems (project) sponsors or chief advocates. They normally are responsible for initiating and funding projects to develop, operate and maintain information systems. System users are the individuals who use or are affected by the information system. Their requirements are crucial in the testing stage of a project. System designers translate business requirements and constraints into technical solutions. System builders construct the system based on the specifications from the systems designers. In most cases, the designers and builders are one and the same.

NEW QUESTION 408

- (Topic 4)

An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?

- A. Consider feasibility of a separate user acceptance environment
- B. Schedule user testing to occur at a given time each day
- C. implement a source code version control tool
- D. Only retest high priority defects

Answer: A

Explanation:

A separate environment or environments is normally necessary for testing to be efficient and effective, and to ensure the integrity of production code, it is important that the development and testing code base be separate. When defects are identified they can be fixed in the development environment, without interrupting testing, before being migrated in a controlled manner to the test environment. A separate test environment can also be used as the final staging area from which code is migrated to production. This enforces a separation between development and production code. The logistics of setting up and refreshing customized test data is easier if a separate environment is maintained. If developers and testers are sharing the same environment, they have to work effectively at separate times of the day. It is unlikely that this would provide optimum productivity. Use of a source code control tool is a good practice, but it does not properly mitigate the lack of an appropriate testing environment. Even low priority fixes run the risk of introducing unintended results when combined with the rest of the system code. To prevent this, regular regression testing covering all code changes should occur. A separate test environment makes the logistics of regression testing easier to manage.

NEW QUESTION 409

- (Topic 4)

At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

- A. report the error as a finding and leave further exploration to the auditee's discretion
- B. attempt to resolve the error
- C. recommend that problem resolution be escalated
- D. ignore the error, as it is not possible to get objective evidence for the software error

Answer: C

Explanation:

When an IS auditor observes such conditions, it is best to fully apprise the auditee and suggest that further problem resolutions be attempted. Recording it as a minor error and leaving it to the auditee's discretion would be inappropriate, and neglecting the error would indicate that the auditor has not taken steps to further probe the issue to its logical end.

NEW QUESTION 412

- (Topic 4)

Which of the following would impair the independence of a quality assurance team?

- A. Ensuring compliance with development methods
- B. Checking the testing assumptions
- C. Correcting coding errors during the testing process
- D. Checking the code to ensure proper documentation

Answer: C

Explanation:

Correction of code should not be a responsibility of the quality assurance team as it would not ensure segregation of duties and would impair the team's independence. The other choices are valid quality assurance functions.

NEW QUESTION 416

- (Topic 4)

From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:

- A. a big bang deployment after proof of concept
- B. prototyping and a one-phase deployment
- C. a deployment plan based on sequenced phases
- D. to simulate the new infrastructure before deployment

Answer: C

Explanation:

When developing a large and complex IT infrastructure, the best practice is to use a phased approach to fitting the entire system together. This will provide greater assurance of quality results. The other choices are riskier approaches.

NEW QUESTION 421

- (Topic 4)

An organization is migrating from a legacy system to an enterprise resource planning (ERP) system. While reviewing the data migration activity, the MOST important concern for the IS auditor is to determine that there is a:

- A. correlation of semantic characteristics of the data migrated between the two systems
- B. correlation of arithmetic characteristics of the data migrated between the two systems
- C. correlation of functional characteristics of the processes between the two systems
- D. relative efficiency of the processes between the two systems

Answer: A

Explanation:

Due to the fact that the two systems could have a different data representation, including the database schema, the IS auditor's main concern should be to verify that the interpretation of the data is the same in the new as it was in the old system. Arithmetic characteristics represent aspects of data structure and internal definition in the database, and therefore are less important than the semantic characteristics. A review of the correlation of the functional characteristics or a review of the relative efficiencies of the processes between the two systems is not relevant to a data migration review.

NEW QUESTION 425

- (Topic 4)

Which of the following would help to ensure the portability of an application connected to a database?

- A. Verification of database import and export procedures
- B. Usage of a structured query language (SQL)
- C. Analysis of stored procedures/triggers
- D. Synchronization of the entity-relation model with the database physical schema

Answer: B

Explanation:

The use of SQL facilitates portability. Verification of import and export procedures with other systems ensures better interfacing with other systems, analyzing stored procedures/triggers ensures proper access/performance, and reviewing the design entity-relation model will be helpful, but none of these contribute to the portability of an application connecting to a database.

NEW QUESTION 426

- (Topic 4)

A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following

would be an IS auditor's main concern about the new process?

- A. Whether key controls are in place to protect assets and information resources
- B. If the system addresses corporate customer requirements
- C. Whether the system can meet the performance goals (time and resources)
- D. Whether owners have been identified who will be responsible for the process

Answer: A

Explanation:

The audit team must advocate the inclusion of the key controls and verify that the controls are in place before implementing the new process. Choices B, C and D are objectives that the business process reengineering (BPR) process should achieve, but they are not the auditor's primary concern.

NEW QUESTION 429

- (Topic 4)

When two or more systems are integrated, input/output controls must be reviewed by an IS auditor in the:

- A. systems receiving the output of other system
- B. systems sending output to other system
- C. systems sending and receiving data
- D. interfaces between the two system

Answer: C

Explanation:

Both of the systems must be reviewed for input/output controls, since the output for one system is the input for the other.

NEW QUESTION 431

.....

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 First Try
- * CISA Practice Test Questions in Multiple Choice Formats and Updates for 1 Year