

CISA Dumps

Isaca CISA

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



NEW QUESTION 1

- (Topic 1)

IS management has decided to rewrite a legacy customer relations system using fourth generation languages (4GLs). Which of the following risks is MOST often associated with system development using 4GLs?

- A. Inadequate screen/report design facilities
- B. Complex programming language subsets
- C. Lack of portability across operating systems
- D. Inability to perform data intensive operations

Answer: D

Explanation:

4GLs are usually not suitable for data intensive operations. Instead, they are used mainly for graphic user interface (GUI) design or as simple query/report generators.

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)

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

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

Answer: B

Explanation:

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

NEW QUESTION 4

- (Topic 1)

Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

- A. Check digit
- B. Existence check
- C. Completeness check
- D. Reasonableness check

Answer: C

Explanation:

A completeness check is used to determine if a field contains data and not zeros or blanks.

NEW QUESTION 5

- (Topic 1)

Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

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

Answer: B

Explanation:

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

NEW QUESTION 6

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 7

- (Topic 1)

Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

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

Answer: A

Explanation:

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

NEW QUESTION 8

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 9

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 10

- (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 10

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 15

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 20

- (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 25

- (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 30

- (Topic 1)

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

- A. Detective

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

Answer: D

Explanation:

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

NEW QUESTION 31

- (Topic 1)

If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

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

Answer: C

Explanation:

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

NEW QUESTION 33

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 36

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 38

- (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 42

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 46

- (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 50

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 53

- (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 54

- (Topic 1)

Which of the following is a guiding best practice for implementing logical access controls?

- A. Implementing the Biba Integrity Model
- B. Access is granted on a least-privilege basis, per the organization's data owners
- C. Implementing the Take-Grant access control model
- D. Classifying data according to the subject's requirements

Answer: B

Explanation:

Logical access controls should be reviewed to ensure that access is granted on a least-privilege basis, per the organization's data owners.

NEW QUESTION 55

- (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 60

- (Topic 1)

Which of the following do digital signatures provide?

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

Answer: A

Explanation:

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

NEW QUESTION 65

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 67

- (Topic 1)

Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

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

Answer: A

Explanation:

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

NEW QUESTION 69

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 73

- (Topic 1)

Which of the following is used to evaluate biometric access controls?

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

Answer: B

Explanation:

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

NEW QUESTION 74

- (Topic 1)

Which of the following is MOST critical during the business impact assessment phase of business continuity planning?

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

Answer: A

Explanation:

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

NEW QUESTION 78

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 79

- (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 81

- (Topic 1)

What is the first step in a business process re-engineering project?

- A. Identifying current business processes
- B. Forming a BPR steering committee
- C. Defining the scope of areas to be reviewed
- D. Reviewing the organizational strategic plan

Answer: C

Explanation:

Defining the scope of areas to be reviewed is the first step in a business process re-engineering project.

NEW QUESTION 84

- (Topic 1)

Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

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

Answer: A

Explanation:

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

NEW QUESTION 89

- (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 94

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 97

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 100

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 101

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 105

- (Topic 1)

What type of risk is associated with authorized program exits (trap doors)? Choose the BEST answer.

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

Answer: D

Explanation:

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

NEW QUESTION 110

- (Topic 1)

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

- A. True
- B. False

Answer: B

Explanation:

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

NEW QUESTION 113

- (Topic 1)

When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.

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

Answer: D

Explanation:

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

NEW QUESTION 118

- (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 123

- (Topic 1)

Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

- A. True
- B. False

Answer: A

Explanation:

Proper segregation of duties prevents a computer operator (user) from performing security administration duties.

NEW QUESTION 128

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 132

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 137

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 141

- (Topic 1)

What are trojan horse programs? Choose the BEST answer.

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

Answer: D

Explanation:

Trojan horse programs are a common form of Internet attack.

NEW QUESTION 145

- (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 148

- (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 151

- (Topic 1)

What is often assured through table link verification and reference checks?

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

Answer: A

Explanation:

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

NEW QUESTION 155

- (Topic 1)

What should IS auditors always check when auditing password files?

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

Answer: B

Explanation:

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

NEW QUESTION 157

- (Topic 1)

Using the OSI reference model, what layer(s) is/are used to encrypt data?

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

Answer: C

Explanation:

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

NEW QUESTION 161

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 162

- (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 163

- (Topic 1)

If a database is restored from information backed up before the last system image, which of the following is recommended?

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

Answer: B

Explanation:

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

NEW QUESTION 168

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 173

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 178

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 181

- (Topic 1)

What is used as a control to detect loss, corruption, or duplication of data?

- A. Redundancy check
- B. Reasonableness check
- C. Hash totals
- D. Accuracy check

Answer: C

Explanation:

Hash totals are used as a control to detect loss, corruption, or duplication of data.

NEW QUESTION 182

- (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 183

- (Topic 1)

Processing controls ensure that data is accurate and complete, and is processed only through which of the following? Choose the BEST answer.

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

Answer: B

Explanation:

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

NEW QUESTION 186

- (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 187

- (Topic 2)

Overall business risk for a particular threat can be expressed as:

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

Answer: A

Explanation:

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

NEW QUESTION 192

- (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 193

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 196

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 198

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 203

- (Topic 2)

The extent to which data will be collected during an IS audit should be determined based on the:

- A. availability of critical and required information
- B. auditor's familiarity with the circumstance
- C. auditee's ability to find relevant evidence
- D. purpose and scope of the audit being done

Answer: D

Explanation:

The extent to which data will be collected during an IS audit should be related directly to the scope and purpose of the audit. An audit with a narrow purpose and scope would result most likely in less data collection, than an audit with a wider purpose and scope. The scope of an IS audit should not be constrained by the ease of obtaining the information or by the auditor's familiarity with the area being audited. Collecting all the required evidence is a required element of an IS audit, and the scope of the audit should not be limited by the auditee's ability to find relevant evidence.

NEW QUESTION 206

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 210

- (Topic 2)

An IS auditor evaluating logical access controls should FIRST:

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

Answer: D

Explanation:

When evaluating logical access controls, an IS auditor should first obtain an understanding of the security risks facing information processing by reviewing relevant documentation, by inquiries, and by conducting a risk assessment. Documentation and evaluation is the second step in assessing the adequacy, efficiency and effectiveness, thus identifying deficiencies or redundancy in controls. The third step is to test the access paths to determine if the controls are functioning. Lastly,

the IS auditor evaluates the security environment to assess its adequacy by reviewing the written policies, observing practices and comparing them to appropriate security best practices.

NEW QUESTION 215

- (Topic 2)

An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

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

Answer: D

Explanation:

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

NEW QUESTION 218

- (Topic 2)

An IS auditor has imported data from the client's database. The next step—confirming whether the imported data are complete—is performed by:

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

Answer: A

Explanation:

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

NEW QUESTION 220

- (Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 223

- (Topic 2)

Which of the following would normally be the MOST reliable evidence for an auditor?

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

Answer: A

Explanation:

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

NEW QUESTION 226

- (Topic 2)

When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

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

Answer: A

Explanation:

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

NEW QUESTION 229

- (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 233

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 235

- (Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 238

- (Topic 2)

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

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

Answer: C

Explanation:

An IS auditor should next examine cases where incorrect calculations occurred and confirm the results. After the calculations have been confirmed, further tests can be conducted and reviewed. Report preparation, findings and recommendations would not be made until all results are confirmed.

NEW QUESTION 240

- (Topic 2)

The BEST method of proving the accuracy of a system tax calculation is by:

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

Answer: C

Explanation:

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

NEW QUESTION 242

- (Topic 2)

The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

- A. understand the business process
- B. comply with auditing standard
- C. identify control weaknesses
- D. plan substantive testing

Answer: A

Explanation:

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

NEW QUESTION 244

- (Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 247

- (Topic 2)

Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

- A. Test data run
- B. Code review
- C. Automated code comparison
- D. Review of code migration procedures

Answer: C

Explanation:

An automated code comparison is the process of comparing two versions of the same program to determine whether the two correspond. It is an efficient technique because it is an automated procedure. Test data runs permit the auditor to verify the processing of preselected transactions, but provide no evidence about unexercised portions of a program. Code review is the process of reading program source code listings to determine whether the code contains potential errors or inefficient statements. A code review can be used as a means of code comparison but it is inefficient. The review of code migration procedures would not detect program changes.

NEW QUESTION 250

- (Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 252

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 253

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 254

- (Topic 2)

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

- A. audit committe
- B. auditee's manage
- C. IS audito
- D. CEO of the organization

Answer: C

Explanation:

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

NEW QUESTION 256

- (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 258

- (Topic 2)

Which of the following is the key benefit of control self-assessment (CSA)?

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

Answer: A

Explanation:

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

NEW QUESTION 260

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 263

- (Topic 3)

Which of the following is a function of an IS steering committee?

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

Answer: C

Explanation:

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

NEW QUESTION 266

- (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 271

- (Topic 3)

From a control perspective, the key element in job descriptions is that they:

- A. provide instructions on how to do the job and define authority
- B. are current, documented and readily available to the employee
- C. communicate management's specific job performance expectation
- D. establish responsibility and accountability for the employee's action

Answer: D

Explanation:

From a control perspective, a job description should establish responsibility and accountability. This will aid in ensuring that users are given system access in accordance with their defined job responsibilities. The other choices are not directly related to controls. Providing instructions on how to do the job and defining authority addresses the managerial and procedural aspects of the job. It is important that job descriptions are current, documented and readily available to the employee, but this in itself is not a control. Communication of management's specific expectations for job performance outlines the standard of performance and would not necessarily include controls.

NEW QUESTION 276

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 277

- (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 282

- (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 286

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 288

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 289

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 291

- (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 294

- (Topic 3)

In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

- A. there is an integration of IS and business staffs within project
- B. there is a clear definition of the IS mission and visio
- C. a strategic information technology planning methodology is in plac
- D. the plan correlates business objectives to IS goals and objective

Answer: A

Explanation:

The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C and D are areas covered by a strategic plan.

NEW QUESTION 296

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 298

- (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 needs
- B. plans are consistent with management strategy
- C. uses its equipment and personnel efficiently and effectively
- 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 302

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 306

- (Topic 3)

In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

- A. implementation
- B. compliance
- C. documentation
- D. sufficiency

Answer: D

Explanation:

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

NEW QUESTION 311

- (Topic 3)

IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

- A. desired result or purpose of implementing specific control procedure
- B. best IT security control practices relevant to a specific entity
- C. techniques for securing information
- D. security policy

Answer: A

Explanation:

An IT control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. They provide the actual objectives for implementing controls and may or may not be the best practices. Techniques are the means of achieving an objective, and a security policy is a subset of IT control objectives.

NEW QUESTION 313

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 314

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 319

- (Topic 3)

Which of the following BEST supports the prioritization of new IT projects?

- A. Internal control self-assessment (CSA)
- B. Information systems audit
- C. Investment portfolio analysis
- D. Business risk assessment

Answer: C

Explanation:

It is most desirable to conduct an investment portfolio analysis, which will present not only a clear focus on investment strategy, but will provide the rationale for terminating nonperforming IT projects. Internal control self-assessment (CSA) may highlight noncompliance to the current policy, but may not necessarily be the best source for driving the prioritization of IT projects. Like internal CSA, IS audits may provide only part of the picture for the prioritization of IT projects. Business risk analysis is part of the investment portfolio analysis but, by itself, is not the best method for prioritizing new IT projects.

NEW QUESTION 323

- (Topic 3)

Which of the following is the BEST information source for management to use as an aid in the identification of assets that are subject to laws and regulations?

- A. Security incident summaries
- B. Vendor best practices
- C. CERT coordination center
- D. Significant contracts

Answer: D

Explanation:

Contractual requirements are one of the sources that should be consulted to identify the requirements for the management of information assets. Vendor best practices provides a basis for evaluating how competitive an enterprise is, while security incident summaries are a source for assessing the vulnerabilities associated with the IT infrastructure. CERT (www.cert.org) is an information source for assessing vulnerabilities within the IT infrastructure.

NEW QUESTION 324

- (Topic 3)

Which of the following is a mechanism for mitigating risks?

- A. Security and control practices
- B. Property and liability insurance

- C. Audit and certification
- D. Contracts and service level agreements (SLAs)

Answer: A

Explanation:

Risks are mitigated by implementing appropriate security and control practices. Insurance is a mechanism for transferring risk. Audit and certification are mechanisms of risk assurance, while contracts and SLAs are mechanisms of risk allocation.

NEW QUESTION 326

- (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 328

- (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 331

- (Topic 3)

An IS auditor reviewing the risk assessment process of an organization should FIRST:

- A. identify the reasonable threats to the information asset
- B. analyze the technical and organizational vulnerabilities
- C. identify and rank the information asset
- D. evaluate the effect of a potential security breach

Answer: C

Explanation:

Identification and ranking of information assets-e.g., data criticality, locations of assets-will set the tone or scope of how to assess risk in relation to the organizational value of the asset. Second, the threats facing each of the organization's assets should be analyzed according to their value to the organization. Third, weaknesses should be identified so that controls can be evaluated to determine if they mitigate the weaknesses. Fourth, analyze how these weaknesses, in absence of given controls, would impact the organization information assets.

NEW QUESTION 332

- (Topic 3)

Which of the following should be the MOST important consideration when deciding areas of priority for IT governance implementation?

- A. Process maturity
- B. Performance indicators
- C. Business risk
- D. Assurance reports

Answer: C

Explanation:

Priority should be given to those areas which represent a known risk to the enterprise's operations. The level of process maturity, process performance and audit reports will feed into the decision making process. Those areas that represent real risk to the business should be given priority.

NEW QUESTION 334

- (Topic 3)

An IS auditor who is reviewing incident reports discovers that, in one instance, an important document left on an employee's desk was removed and put in the garbage by the outsourced cleaning staff. Which of the following should the IS auditor recommend to management?

- A. Stricter controls should be implemented by both the organization and the cleaning agency
- B. No action is required since such incidents have not occurred in the past
- C. A clear desk policy should be implemented and strictly enforced in the organization
- D. A sound backup policy for all important office documents should be implemented

Answer: A

Explanation:

An employee leaving an important document on a desk and the cleaning staff removing it may result in a serious impact on the business. Therefore, the IS auditor should recommend that strict controls be implemented by both the organization and the outsourced cleaning agency. That such incidents have not occurred in the past does not reduce the seriousness of their impact. Implementing and monitoring a clear desk policy addresses only one part of the issue. Appropriate confidentiality agreements with the cleaning agency, along with ensuring that the cleaning staff has been educated on the dos and don'ts of the cleaning process, are also controls that should be implemented. The risk here is not a loss of data, but leakage of data to unauthorized sources. A backup policy does not address the issue of unauthorized leakage of information.

NEW QUESTION 336

- (Topic 3)

The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

- A. financial result
- B. customer satisfaction
- C. internal process efficiency
- D. innovation capacity

Answer: A

Explanation:

Financial results have traditionally been the sole overall performance metric. The IT balanced scorecard (BSC) is an IT business governance tool aimed at monitoring IT performance evaluation indicators other than financial results. The IT BSC considers other key success factors, such as customer satisfaction, innovation capacity and processing.

NEW QUESTION 339

- (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 functionality

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 343

- (Topic 4)

Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

- A. Function point analysis
- B. PERT chart
- C. Rapid application development
- D. Object-oriented system development

Answer: B

Explanation:

A PERT chart will help determine project duration once all the activities and the work involved with those activities are known. Function point analysis is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal files, etc. While this will help determine the size of individual activities, it will not assist in determining project duration since there are many overlapping tasks. Rapid application development is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality, while object-oriented system development is the process of solution specification and modeling.

NEW QUESTION 344

- (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 347

- (Topic 4)

At the completion of a system development project, a postproject review should include which of the following?

- A. Assessing risks that may lead to downtime after the production release
- B. Identifying lessons learned that may be applicable to future projects
- C. Verifying the controls in the delivered system are working
- D. Ensuring that test data are deleted

Answer: B

Explanation:

A project team has something to learn from each and every project. As risk assessment is a key issue for project management, it is important for the organization to accumulate lessons learned and integrate them into future projects. An assessment of potential downtime should be made with the operations group and other specialists before implementing a system. Verifying that controls are working should be covered during the acceptance test phase and possibly, again, in the postimplementation review. Test data should be retained for future regression testing.

NEW QUESTION 350

- (Topic 4)

An IS auditor is assigned to audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

- A. Report that the organization does not have effective project management
- B. Recommend the project manager be changed
- C. Review the IT governance structure
- D. Review the conduct of the project and the business case

Answer: D

Explanation:

Before making any recommendations, an IS auditor needs to understand the project and the factors that have contributed to making the project over budget and over schedule. The organization may have effective project management practices and sound IT governance and still be behind schedule or over budget. There is no indication that the project manager should be changed without looking into the reasons for the overrun.

NEW QUESTION 354

- (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 357

- (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 resolve
- B. recommend that compensating controls be implemente
- 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 360

- (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 362

- (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 364

- (Topic 4)

Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

- A. Check digit
- B. Existence check
- C. Completeness check
- D. Reasonableness check

Answer: C

Explanation:

A completeness check is used to determine if a field contains data and not zeros or blanks. A check digit is a digit calculated mathematically to ensure original data were not altered. An existence check also checks entered data for agreement to predetermined criteria. A reasonableness check matches input to predetermined reasonable limits or occurrence rates.

NEW QUESTION 368

- (Topic 4)

The editing/validation of data entered at a remote site would be performed MOST effectively at the:

- A. central processing site after running the application syste
- B. central processing site during the running of the application syste
- C. remote processing site after transmission of the data to the central processing sit
- D. remote processing site prior to transmission of the data to the central processing sit

Answer: D

Explanation:

It is important that the data entered from a remote site is edited and validated prior to transmission to the central processing site.

NEW QUESTION 370

- (Topic 4)

What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

- A. Test data/deck
- B. Base-case system evaluation
- C. Integrated test facility (ITF)
- D. Parallel simulation

Answer: B

Explanation:

A base-case system evaluation uses test data sets developed as part of comprehensive testing programs, it is used to verify correct systems operations before acceptance, as well as periodic validation. Test data/deck simulates transactions through real programs. An ITF creates fictitious files in the database with test transactions processed simultaneously with live input. Parallel simulation is the production of data processed using computer programs that simulate application program logic.

NEW QUESTION 371

- (Topic 4)

What control detects transmission errors by appending calculated bits onto the end of each segment of data?

- A. Reasonableness check
- B. Parity check
- C. Redundancy check
- D. Check digits

Answer: C

Explanation:

A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of data. A reasonableness check compares data to predefined reasonability limits or occurrence rates established for the data. A parity check is a hardware control that detects data errors when data are read from one computer to another, from memory or during transmission. Check digits detect transposition and transcription errors.

NEW QUESTION 374

- (Topic 4)

Which of the following is the GREATEST risk when implementing a data warehouse?

- A. increased response time on the production systems
- B. Access controls that are not adequate to prevent data modification
- C. Data duplication
- D. Data that is not updated or current

Answer: B

Explanation:

Once the data is in a warehouse, no modifications should be made to it and access controls should be in place to prevent data modification. Increased response time on the production systems is not a risk, because a data warehouse does not impact production data. Based on data replication, data duplication is inherent in a data warehouse. Transformation of data from operational systems to a data warehouse is done at predefined intervals, and as such, data may not be current.

NEW QUESTION 379

- (Topic 4)

An appropriate control for ensuring the authenticity of orders received in an EDI application is to:

- A. acknowledge receipt of electronic orders with a confirmation message
- B. perform reasonableness checks on quantities ordered before filling order
- C. verify the identity of senders and determine if orders correspond to contract terms
- D. encrypt electronic order

Answer: C

Explanation:

An electronic data interchange (EDI) system is subject not only to the usual risk exposures of computer systems but also to those arising from the potential ineffectiveness of controls on the part of the trading partner and the third-party service provider, making authentication of users and messages a major security concern. Acknowledging the receipt of electronic orders with a confirming message is good practice but will not authenticate orders from customers. Performing reasonableness checks on quantities ordered before placing orders is a control for ensuring the correctness of the company's orders, not the authenticity of its customers' orders. Encrypting sensitive messages is an appropriate step but does not apply to messages received.

NEW QUESTION 382

- (Topic 4)

Failure in which of the following testing stages would have the GREATEST impact on the implementation of new application software?

- A. System testing
- B. Acceptance testing
- C. Integration testing
- D. Unit testing

Answer: B

Explanation:

Acceptance testing is the final stage before the software is installed and is available for use. The greatest impact would occur if the software fails at the acceptance testing level, as this could result in delays and cost overruns. System testing is undertaken by the developer team to determine if the software meets user requirements per specifications. Integration testing examines the units/modules as one integrated system and unit testing examines the individual units or components of the software. System, integration and unit testing are all performed by the developers at various stages of development; the impact of failure is comparatively less for each than failure at the acceptance testing stage.

NEW QUESTION 387

- (Topic 4)

An organization has an integrated development environment (IDE) on which the program libraries reside on the server, but modification/development and testing are done from PC workstations. Which of the following would be a strength of an IDE?

- A. Controls the proliferation of multiple versions of programs
- B. Expands the programming resources and aids available
- C. Increases program and processing integrity
- D. Prevents valid changes from being overwritten by other changes

Answer: B

Explanation:

A strength of an IDE is that it expands the programming resources and aids available. The other choices are IDE weaknesses.

NEW QUESTION 389

- (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 393

- (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 projec
- 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 394

- (Topic 4)

A decision support system (DSS):

- A. is aimed at solving highly structured problem
- B. combines the use of models with nontraditional data access and retrieval function
- C. emphasizes flexibility in the decision making approach of user
- D. supports only structured decision making task

Answer: C

Explanation:

DSS emphasizes flexibility in the decision making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions, and supports semistructured decision making tasks.

NEW QUESTION 399

- (Topic 4)

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

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

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 400

- (Topic 4)

When a new system is to be implemented within a short time frame, it is MOST important to:

- A. finish writing user manual
- B. perform user acceptance testin
- C. add last-minute enhancements to functionalitie
- D. ensure that the code has been documented and reviewe

Answer: B

Explanation:

It would be most important to complete the user acceptance testing to ensure that the system to be implemented is working correctly. The completion of the user manuals is similar to the performance of code reviews. If time is tight, the last thing one would want to do is add another enhancement, as it would be necessary to freeze the code and complete the testing, then make any other changes as future enhancements. It would be appropriate to have the code documented and reviewed, but unless the acceptance testing is completed, there is no guarantee that the system will work correctly and meet user requirements.

NEW QUESTION 402

- (Topic 4)

The MOST likely explanation for the use of applets in an Internet application is that:

- A. it is sent over the network from the serve
- B. the server does not run the program and the output is not sent over the networ
- C. they improve the performance of the web server and network
- D. it is a JAVA program downloaded through the web browser and executed by the web server of the client machin

Answer: C

Explanation:

An applet is a JAVA program that is sent over the network from the web server, through a web browser and to the client machine; the code is then run on the machine. Since the server does not run the program and the output is not sent over the network, the performance on the web server and network-over which the server and client are connected-dramatically improves through the use of applets. Performance improvement is more important than the reasons offered in choices A and B. Since JAVA virtual machine (JVM) is embedded in most web browsers, the applet download through the web browser runs on the client machine from the web browser, not from the web server, making choice D incorrect.

NEW QUESTION 407

- (Topic 4)

Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

- A. Intrusion detection systems
- B. Data mining techniques
- C. Firewalls
- D. Packet filtering routers

Answer: B

Explanation:

Data mining is a technique used to detect trends or patterns of transactions or data. If the historical pattern of charges against a credit card account is changed, then it is a flag that the transaction may have resulted from a fraudulent use of the card.

NEW QUESTION 412

- (Topic 4)

During the requirements definition phase of a software development project, the aspects of software testing that should be addressed are developing:

- A. test data covering critical application
- B. detailed test plan

- C. quality assurance test specification
- D. user acceptance testing specification

Answer: D

Explanation:

A key objective in any software development project is to ensure that the developed software will meet the business objectives and the requirements of the user. The users should be involved in the requirements definition phase of a development project and user acceptance test specification should be developed during this phase. The other choices are generally performed during the system testing phase.

NEW QUESTION 413

- (Topic 4)

Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?

- A. Applications may not be subject to testing and IT general controls
- B. increased development and maintenance costs
- C. increased application development time
- D. Decision-making may be impaired due to diminished responsiveness to requests for information

Answer: A

Explanation:

End-user developed applications may not be subjected to an independent outside review by systems analysts and frequently are not created in the context of a formal development methodology. These applications may lack appropriate standards, controls, quality assurance procedures, and documentation. A risk of end-user applications is that management may rely on them as much as traditional applications. End-user computing (EUC) systems typically result in reduced application development and maintenance costs, and a reduced development cycle time. EUC systems normally increase flexibility and responsiveness to management's information requests.

NEW QUESTION 418

- (Topic 4)

The MAJOR advantage of a component-based development approach is the:

- A. ability to manage an unrestricted variety of data type
- B. provision for modeling complex relationship
- C. capacity to meet the demands of a changing environmen
- D. support of multiple development environment

Answer: D

Explanation:

Components written in one language can interact with components written in other languages or running on other machines, which can increase the speed of development. Software developers can then focus on business logic. The other choices are not the most significant advantages of a component-based development approach.

NEW QUESTION 422

- (Topic 4)

Following best practices, formal plans for implementation of new information systems are developed during the:

- A. development phas
- B. design phas
- C. testing phas
- D. deployment phas

Answer: B

Explanation:

Planning for implementation should begin well in advance of the actual implementation date. A formal implementation plan should be constructed in the design phase and revised as the development progresses.

NEW QUESTION 423

- (Topic 4)

An IS auditor is reviewing a project that is using an Agile software development approach. Which of the following should the IS auditor expect to find?

- A. Use of a process-based maturity model such as the capability maturity model (CMM)
- B. Regular monitoring of task-level progress against schedule
- C. Extensive use of software development tools to maximize team productivity
- D. Postiteration reviews that identify lessons learned for future use in the project

Answer: D

Explanation:

A key tenet of the Agile approach to software project management is team learning and the use of team learning to refine project management and software development processes as the project progresses. One of the best ways to achieve this is that, at the end of each iteration, the team considers and documents

what worked well and what could have worked better, and identifies improvements to be implemented in subsequent iterations. CMM and Agile really sit at opposite poles. CMM places heavy emphasis on predefined formal processes and formal project management and software development deliverables. Agile projects, by contrast, rely on refinement of process as dictated by the particular needs of the project and team dynamics. Additionally, less importance is placed on formal paper-based deliverables, with the preference being effective informal communication within the team and with key outside contributors. Agile projects produce releasable software in short iterations, typically ranging from 4 to 8 weeks. This, in itself, instills considerable performance discipline within the team. This, combined with short daily meetings to agree on what the team is doing and the identification of any impediments, renders task-level tracking against a schedule redundant. Agile projects do make use of suitable development tools; however, tools are not seen as the primary means of achieving productivity. Team harmony, effective communications and collective ability to solve challenges are of

NEW QUESTION 426

- (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 concep
- B. prototyping and a one-phase deploymen
- C. a deployment plan based on sequenced phase
- D. to simulate the new infrastructure before deploymen

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 427

- (Topic 4)

During a postimplementation review of an enterprise resource management system, an IS auditor would MOST likely:

- A. review access control configuratio
- B. evaluate interface testin
- C. review detailed design documentatio
- D. evaluate system testin

Answer: A

Explanation:

Reviewing access control configuration would be the first task performed to determine whether security has been appropriately mapped in the system. Since a postimplementation review is done after user acceptance testing and actual implementation, onewould not engage in interface testing or detailed design documentation. Evaluating interface testing would be part of the implementation process. The issue of reviewing detailed design documentation is not generally relevant to an enterprise resource management system, since these are usually vendor packages with user manuals. System testing should be performed before final user signoff.

NEW QUESTION 428

- (Topic 4)

During an application audit, an IS auditor finds several problems related to corrupted data in the database. Which of the following is a corrective control that the IS auditor should recommend?

- A. implement data backup and recovery procedure
- B. Define standards and closely monitor for complianc
- C. Ensure that only authorized personnel can update the databas
- D. Establish controls to handle concurrent access problem

Answer: A

Explanation:

Implementing data backup and recovery procedure is a corrective control, because backup and recovery procedures can be used to roll back database errors. Defining or establishing standards is a preventive control, while monitoring for compliance is adetective control. Ensuring that only authorized personnel can update the database is a preventive control. Establishing controls to handle concurrent access problems is also a preventive control.

NEW QUESTION 430

- (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 434

- (Topic 4)

Business units are concerned about the performance of a newly implemented system. Which of the following should an IS auditor recommend?

- A. Develop a baseline and monitor system usage
- B. Define alternate processing procedure
- C. Prepare the maintenance manual
- D. Implement the changes users have suggested

Answer: A

Explanation:

An IS auditor should recommend the development of a performance baseline and monitor the system's performance, against the baseline, to develop empirical data upon which decisions for modifying the system can be made. Alternate processing procedures and a maintenance manual will not alter a system's performance. Implementing changes without knowledge of the cause(s) for the perceived poor performance may not result in a more efficient system.

NEW QUESTION 435

- (Topic 4)

An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would MOST likely:

- A. check to ensure that the type of transaction is valid for the card type
- B. verify the format of the number entered then locate it on the database
- C. ensure that the transaction entered is within the cardholder's credit limit
- D. confirm that the card is not shown as lost or stolen on the master file

Answer: B

Explanation:

The initial validation should confirm whether the card is valid. This validity is established through the card number and PIN entered by the user. Based on this initial validation, all other validations will proceed. A validation control in data capture will ensure that the data entered is valid (i.e., it can be processed by the system). If the data captured in the initial validation is not valid (if the card number or PIN do not match with the database), then the card will be rejected or captured per the controls in place. Once initial validation is completed, then other validations specific to the card and cardholder would be performed.

NEW QUESTION 438

- (Topic 4)

A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:

- A. payroll reports should be compared to input form
- B. gross payroll should be recalculated manually
- C. checks (cheques) should be compared to input form
- D. checks (cheques) should be reconciled with output report

Answer: A

Explanation:

The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports. Hence, comparing payroll reports with input forms is the best mechanism of verifying data accuracy. Recalculating gross payroll manually would only verify whether the processing is correct and not the data accuracy of inputs. Comparing checks (cheques) to input forms is not feasible as checks (cheques) have the processed information and input forms have the input data. Reconciling checks (cheques) with output reports only confirms that checks (cheques) have been issued as per output reports.

NEW QUESTION 440

- (Topic 4)

Which of the following represents the GREATEST potential risk in an EDI environment?

- A. Transaction authorization
- B. Loss or duplication of EDI transmissions
- C. Transmission delay
- D. Deletion or manipulation of transactions prior to or after establishment of application controls

Answer: A

Explanation:

Since the interaction between parties is electronic, there is no inherent authentication occurring; therefore, transaction authorization is the greatest risk. Choices B and D are examples of risks, but the impact is not as great as that of unauthorized transactions. Transmission delays may terminate the process or hold the line until the normal time for processing has elapsed; however, there will be no loss of data.

NEW QUESTION 445

- (Topic 4)

When using an integrated test facility (ITF), an IS auditor should ensure that:

- A. production data are used for testing
- B. test data are isolated from production data

- C. a test data generator is use
- D. master files are updated with the test dat

Answer: B

Explanation:

An integrated test facility (ITF) creates a fictitious file in the database, allowing for test transactions to be processed simultaneously with live data. While this ensures that periodic testing does not require a separate test process, there is a need to isolate test data from production data. An IS auditor is not required to use production data or a test data generator. Production master files should not be updated with test data.

NEW QUESTION 450

- (Topic 4)

A clerk changed the interest rate for a loan on a master file. The rate entered is outside the normal range for such a loan. Which of the following controls is MOST effective in providing reasonable assurance that the change was authorized?

- A. The system will not process the change until the clerk's manager confirms the change by entering an approval code
- B. The system generates a weekly report listing all rate exceptions and the report is reviewed by the clerk's manager
- C. The system requires the clerk to enter an approval code
- D. The system displays a warning message to the clerk

Answer: A

Explanation:

Choice A would prevent or detect the use of an unauthorized interest rate. Choice B informs the manager after the fact that a change was made, thereby making it possible for transactions to use an unauthorized rate prior to management review. Choices C and D do not prevent the clerk from entering an unauthorized rate change.

NEW QUESTION 452

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 455

- (Topic 4)

When performing an audit of a client relationship management (CRM) system migration project, which of the following should be of GREATEST concern to an IS auditor?

- A. The technical migration is planned for a Friday preceding a long weekend, and the time window is too short for completing all tasks
- B. Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old system
- C. A single implementation is planned, immediately decommissioning the legacy system
- D. Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's software

Answer: C

Explanation:

Major system migrations should include a phase of parallel operation or a phased cut-over to reduce implementation risks. Decommissioning or disposing of the old hardware would complicate any fallback strategy, should the new system not operate correctly. A weekend can be used as a time buffer so that the new system will have a better chance of being up and running after the weekend. A different data representation does not mean different data presentation at the front end. Even when this is the case, this issue can be solved by adequate training and user support. The printing functionality is commonly one of the last functions to be tested in a new system because it is usually the last step performed in any business event. Thus, meaningful testing and the respective error fixing are only possible after all other parts of the software have been successfully tested.

NEW QUESTION 457

- (Topic 5)

To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?

- A. System access log files
- B. Enabled access control software parameters
- C. Logs of access control violations
- D. System configuration files for control options used

Answer: D

Explanation:

A review of system configuration files for control options used would show which users have access to the privileged supervisory state. Both systems access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

NEW QUESTION 458

- (Topic 5)

Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?

- A. A system downtime log
- B. Vendors' reliability figures
- C. Regularly scheduled maintenance log
- D. A written preventive maintenance schedule

Answer: A

Explanation:

A system downtime log provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

NEW QUESTION 459

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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