

Exam Questions CISA

Isaca CISA

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



NEW QUESTION 1

- (Topic 1)

Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?

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

Answer: D

Explanation:

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

NEW QUESTION 2

- (Topic 1)

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)

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

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

Answer: B

Explanation:

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

NEW QUESTION 4

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 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)

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

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

Answer: A

Explanation:

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

NEW QUESTION 7

- (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 8

- (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 9

- (Topic 1)

A hardware control that helps to detect errors when data are communicated from one computer to another is known as a:

- A. duplicate chec
- B. table looku
- C. validity chec
- D. parity chec

Answer: D

Explanation:

A parity check will help to detect data errors when data are read from memory or communicated from one computer to another. A one-bit digit (either 0 or 1) is added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, an error report is generated.

NEW QUESTION 10

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 10

- (Topic 1)

Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

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

Answer: C

Explanation:

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

NEW QUESTION 14

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 18

- (Topic 1)

What is the PRIMARY purpose of audit trails?

- A. To document auditing efforts
- B. To correct data integrity errors
- C. To establish accountability and responsibility for processed transactions
- D. To prevent unauthorized access to data

Answer: C

Explanation:

The primary purpose of audit trails is to establish accountability and responsibility for processed transactions.

NEW QUESTION 23

- (Topic 1)

The use of statistical sampling procedures helps minimize:

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

Answer: A

Explanation:

The use of statistical sampling procedures helps minimize detection risk.

NEW QUESTION 26

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 30

- (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 35

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 38

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 43

- (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 45

- (Topic 1)

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

- A. Lack of employee awareness of a company's information security policy
- B. Failure to comply with a company's information security policy

- C. A momentary lapse of reason
- D. Lack of security policy enforcement procedures

Answer: A

Explanation:

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

NEW QUESTION 46

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 47

- (Topic 1)

What is essential for the IS auditor to obtain a clear understanding of network management?

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

Answer: C

Explanation:

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

NEW QUESTION 48

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 52

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 53

- (Topic 1)

How does the SSL network protocol provide confidentiality?

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

Answer: D

Explanation:

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

NEW QUESTION 58

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 59

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 62

- (Topic 1)

What are often the primary safeguards for systems software and data?

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

Answer: B

Explanation:

Logical access controls are often the primary safeguards for systems software and data.

Which of the following is often used as a detection and deterrent control against Internet

attacks? A. Honeypots B. CCTV C. VPN D. VLAN Answer: A Honeypots are often used as a detection and deterrent control against Internet attacks.

NEW QUESTION 67

- (Topic 1)

What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources? Choose the BEST answer.

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

Answer: C

Explanation:

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

NEW QUESTION 69

- (Topic 1)

What is the key distinction between encryption and hashing algorithms?

- A. Hashing algorithms ensure data confidentiality
- B. Hashing algorithms are irreversible
- C. Encryption algorithms ensure data integrity

D. Encryption algorithms are not irreversibl

Answer: B

Explanation:

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

NEW QUESTION 74

- (Topic 1)

Establishing data ownership is an important first step for which of the following processes? Choose the BEST answer.

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

Answer: D

Explanation:

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

NEW QUESTION 79

- (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 82

- (Topic 1)

What influences decisions regarding criticality of assets?

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

Answer: C

Explanation:

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

NEW QUESTION 87

- (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 92

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 95

- (Topic 1)

Who assumes ownership of a systems-development project and the resulting system?

- A. User management
- B. Project steering committee
- C. IT management
- D. Systems developers

Answer: A

Explanation:

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

NEW QUESTION 100

- (Topic 1)

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

- A. True
- B. False

Answer: B

Explanation:

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

NEW QUESTION 104

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 107

- (Topic 1)

What must an IS auditor understand before performing an application audit? Choose the BEST answer.

- A. The potential business impact of application risk
- B. Application risks must first be identified
- C. Relative business processes
- D. Relevant application risk

Answer: C

Explanation:

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

NEW QUESTION 109

- (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 113

- (Topic 1)

A check digit is an effective edit check to:

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

Answer: B

Explanation:

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

NEW QUESTION 114

- (Topic 1)

Who should be responsible for network security operations?

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

Answer: B

Explanation:

Security administrators are usually responsible for network security operations.

NEW QUESTION 118

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 123

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 125

- (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 127

- (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 128

- (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 129

- (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 134

- (Topic 1)

What is/are used to measure and ensure proper network capacity management and availability of services? Choose the BEST answer.

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

Answer: A

Explanation:

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

NEW QUESTION 136

- (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 138

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 141

- (Topic 1)

What is a callback system?

- A. It is a remote-access system whereby the remote-access server immediately calls the user back at a predetermined number if the dial-in connection fail
- B. It is a remote-access system whereby the user's application automatically redials the remoteaccess server if the initial connection attempt fail
- C. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration databas
- D. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently allows the user to call back at an approved number for a limited period of tim

Answer: C

Explanation:

A callback system is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.

NEW QUESTION 145

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 147

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 152

- (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 155

- (Topic 1)

What are intrusion-detection systems (IDS) primarily used for?

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

Answer: D

Explanation:

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

NEW QUESTION 158

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 161

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 162

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 165

- (Topic 1)

What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

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

Answer: C

Explanation:

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

NEW QUESTION 167

- (Topic 1)

Who is ultimately responsible for providing requirement specifications to the software-development team?

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

Answer: A

Explanation:

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

NEW QUESTION 169

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 173

- (Topic 1)

Which of the following uses a prototype that can be updated continually to meet changing user or business requirements?

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

Answer: B

Explanation:

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

NEW QUESTION 178

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 182

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 183

- (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 187

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 191

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 193

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 197

- (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 202

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 206

- (Topic 1)

An IS auditor is using a statistical sample to inventory the tape library. What type of test would this be considered?

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

Answer: A

Explanation:

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

NEW QUESTION 211

- (Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 215

- (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 220

- (Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 222

- (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 223

- (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 228

- (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 233

- (Topic 2)

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

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

Answer: B

Explanation:

In developing a risk-based audit strategy, it is critical that the risks and vulnerabilities be understood. This will determine the areas to be audited and the extent of coverage. Understanding whether appropriate controls required to mitigate risks are in place is a resultant effect of an audit. Audit risks are inherent aspects of auditing, are directly related to the audit process and are not relevant to the risk analysis of the environment to be audited. A gap analysis would normally be done to compare the actual state to an expected or desirable state.

NEW QUESTION 238

- (Topic 2)

An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

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

Answer: D

Explanation:

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

NEW QUESTION 239

- (Topic 2)

The PRIMARY purpose of an IT forensic audit is:

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

Answer: B

Explanation:

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

NEW QUESTION 244

- (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 controls

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 247

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 249

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 250

- (Topic 2)

Which of the following forms of evidence for the auditor would be considered the MOST reliable?

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

Answer: D

Explanation:

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

NEW QUESTION 252

- (Topic 2)

An IS auditor reviews an organizational chart PRIMARILY for:

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

Answer: C

Explanation:

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

NEW QUESTION 257

- (Topic 2)

Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

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

Answer: D

Explanation:

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

NEW QUESTION 259

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 262

- (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 264

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 267

- (Topic 2)

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

- A. Personally delete all copies of the unauthorized software

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

Answer: C

Explanation:

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

NEW QUESTION 271

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 272

- (Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 275

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 277

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 280

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 283

- (Topic 3)

The ultimate purpose of IT governance is to:

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

Answer: A

Explanation:

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

NEW QUESTION 288

- (Topic 3)

What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

- A. Repeatable but Intuitive
- B. Defined
- C. Managed and Measurable
- D. Optimized

Answer: B

Explanation:

Defined (level 3) is the lowest level at which an IT balanced scorecard is defined.

NEW QUESTION 290

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 293

- (Topic 3)

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

- A. length of service, since this will help ensure technical competenc
- B. age, as training in audit techniques may be impractica

- C. IS knowledge, since this will bring enhanced credibility to the audit function
- D. ability, as an IS auditor, to be independent of existing IS relationship

Answer: D

Explanation:

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

NEW QUESTION 294

- (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 295

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 296

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 300

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 305

- (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 310

- (Topic 3)

To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

- A. control self-assessment
- B. a business impact analysis
- C. an IT balanced scorecard
- D. business process reengineering

Answer: C

Explanation:

An IT balanced scorecard (BSC) provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. Control self-assessment (CSA), business impact analysis (BIA) and business process reengineering (BPR) are insufficient to align IT with organizational objectives.

NEW QUESTION 312

- (Topic 3)

When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

- A. establishment of a review board
- B. creation of a security unit
- C. effective support of an executive sponsor
- D. selection of a security process owner

Answer: C

Explanation:

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

NEW QUESTION 315

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 319

- (Topic 3)

Which of the following is the initial step in creating a firewall policy?

- A. A cost-benefit analysis of methods for securing the applications
- B. Identification of network applications to be externally accessed
- C. Identification of vulnerabilities associated with network applications to be externally accessed
- D. Creation of an applications traffic matrix showing protection methods

Answer: B

Explanation:

Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in charge will be able to understand the need for, and possible methods of, controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

NEW QUESTION 321

- (Topic 3)

A top-down approach to the development of operational policies will help ensure:

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

Answer: A

Explanation:

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

NEW QUESTION 324

- (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 327

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 329

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 332

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 334

- (Topic 3)

While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern should be that the:

- A. requirement for protecting confidentiality of information could be compromised
- B. contract may be terminated because prior permission from the outsourcer was not obtained
- C. other service provider to whom work has been outsourced is not subject to audit
- D. outsourcer will approach the other service provider directly for further work

Answer: A

Explanation:

Many countries have enacted regulations to protect the confidentiality of information maintained in their countries and/or exchanged with other countries. Where a service provider outsources part of its services to another service provider, there is a potential risk that the confidentiality of the information will be compromised. Choices B and C could be concerns but are not related to ensuring the confidentiality of information. There is no reason why an IS auditor should be concerned with choice D.

NEW QUESTION 335

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 337

- (Topic 3)

An IS auditor is reviewing an IT security risk management program. Measures of security risk should:

- A. address all of the network risk
- B. be tracked over time against the IT strategic plan
- C. take into account the entire IT environment
- D. result in the identification of vulnerability tolerance

Answer: C

Explanation:

When assessing IT security risk, it is important to take into account the entire IT environment. Measures of security risk should focus on those areas with the highest criticality so as to achieve maximum risk reduction at the lowest possible cost. IT strategic plans are not granular enough to provide appropriate measures. Objective metrics must be tracked over time against measurable goals, thus the management of risk is enhanced by comparing today's results against last week, last month, last quarter. Risk measures will profile assets on a network to objectively measure vulnerability risk. They do not identify tolerances.

NEW QUESTION 341

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 342

- (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 344

- (Topic 3)

During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described IT risks. What is the MOST appropriate recommendation in this situation?

- A. Create an IT risk management department and establish an IT risk framework with the aid of external risk management expert
- B. Use common industry standard aids to divide the existing risk documentation into several individual risks which will be easier to handle
- C. No recommendation is necessary since the current approach is appropriate for a medium-sized organization
- D. Establish regular IT risk management meetings to identify and assess risks, and create a mitigation plan as input to the organization's risk management

Answer: D

Explanation:

Establishing regular meetings is the best way to identify and assess risks in a medium-sized organization, to address responsibilities to the respective management and to keep the risk list and mitigation plans up to date. A medium-sized organization would normally not have a separate IT risk management department. Moreover, the risks are usually manageable enough so that external help would not be needed. While common risks may be covered by common industry standards, they cannot address the specific situation of an organization. Individual risks will not be discovered without a detailed assessment from within the organization. Splitting the one risk position into several is not sufficient.

NEW QUESTION 348

- (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 352

- (Topic 4)

To minimize the cost of a software project, quality management techniques should be applied:

- A. as close to their writing (i.e., point of origination) as possible
- B. primarily at project start-up to ensure that the project is established in accordance with organizational governance standard
- C. continuously throughout the project with an emphasis on finding and fixing defects primarily during testing to maximize the defect detection rate
- D. mainly at project close-down to capture lessons learned that can be applied to future project

Answer: C

Explanation:

While it is important to properly establish a software development project, quality management should be effectively practiced throughout the project. The major source of unexpected costs on most software projects is rework. The general rule is that the earlier in the development life cycle that a defect occurs, and the longer it takes to find and fix that defect, the more effort will be needed to correct it. A well-written quality management plan is a good start, but it must also be actively applied. Simply relying on testing to identify defects is a relatively costly and less effective way of achieving software quality. For example, an error in requirements discovered in the testing phase can result in scrapping significant amounts of work. Capturing lessons learned will be too late for the current project. Additionally, applying quality management techniques throughout a project is likely to yield its own insights into the causes of quality problems and assist in staff development.

NEW QUESTION 353

- (Topic 4)

An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

- A. complexity and risks associated with the project have been analyzed
- B. resources needed throughout the project have been determined
- C. project deliverables have been identified
- D. a contract for external parties involved in the project has been completed

Answer: A

Explanation:

Understanding complexity and risk, and actively managing these throughout a project are critical to a successful outcome. The other choices, while important during the course of the project, cannot be fully determined at the time the project is initiated, and are often contingent upon the risk and complexity of the project.

NEW QUESTION 356

- (Topic 4)

Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

- A. Function point analysis
- B. Earned value analysis
- C. Cost budget
- D. Program Evaluation and Review Technique

Answer: B

Explanation:

Earned value analysis (EVA) is an industry standard method for measuring a project's progress at any given point in time, forecasting its completion date and final cost, and analyzing variances in the schedule and budget as the project proceeds. It compares the planned amount of work with what has actually been completed, to determine if the cost, schedule and work accomplished are progressing in accordance with the plan. EVA works most effectively if a well-formed work breakdown structure exists. Function point analysis (FPA) is an indirect measure of software size and complexity and, therefore, does not address the elements of time and budget. Cost budgets do not address time. PERT aids in time and deliverables management, but lacks projections for estimates at completion (EACs) and overall financial management.

NEW QUESTION 357

- (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 358

- (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)

Which of the following techniques would BEST help an IS auditor gain reasonable assurance that a project can meet its target date?

- A. Estimation of the actual end date based on the completion percentages and estimated time to complete, taken from status reports
- B. Confirmation of the target date based on interviews with experienced managers and staff involved in the completion of the project deliverables
- C. Extrapolation of the overall end date based on completed work packages and current resources
- D. Calculation of the expected end date based on current resources and remaining available project budget

Answer: C

Explanation:

Direct observation of results is better than estimations and qualitative information gained from interviews or status reports. Project managers and involved staff tend to underestimate the time needed for completion and the necessary time buffers for dependencies between tasks, while overestimating the completion percentage for tasks underway (80:20 rule). The calculation based on remaining budget does not take into account the speed at which the project has been progressing.

NEW QUESTION 363

- (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 368

- (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 373

- (Topic 4)

To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

- A. during data preparatio
- B. in transit to the compute
- C. between related computer run
- D. during the return of the data to the user departmen

Answer: A

Explanation:

During data preparation is the best answer, because it establishes control at the earliest point.

NEW QUESTION 377

- (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 380

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 382

- (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 387

- (Topic 4)

The MAIN purpose of a transaction audit trail is to:

- A. reduce the use of storage media
- B. determine accountability and responsibility for processed transaction
- C. help an IS auditor trace transaction
- D. provide useful information for capacity planning

Answer: B

Explanation:

Enabling audit trails aids in establishing the accountability and responsibility for processed transactions by tracing them through the information system. Enabling audit trails increases the use of disk space. A transaction log file would be used to trace transactions, but would not aid in determining accountability and responsibility. The objective of capacity planning is the efficient and effective use of IT resources and requires information such as CPU utilization, bandwidth, number of users, etc.

NEW QUESTION 390

- (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 394

- (Topic 4)

The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:

- A. rule
- B. decision tree
- C. semantic net
- D. dataflow diagram

Answer: B

Explanation:

Decision trees use questionnaires to lead a user through a series of choices until a conclusion is reached. Rules refer to the expression of declarative knowledge through the use of if-then relationships. Semantic nets consist of a graph in which nodes represent physical or conceptual objects and the arcs describe the relationship between the nodes. Semantic nets resemble a dataflow diagram and make use of an inheritance mechanism to prevent duplication of data.

NEW QUESTION 399

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 402

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 403

- (Topic 4)

Functionality is a characteristic associated with evaluating the quality of software products throughout their life cycle, and is BEST described as the set of attributes that bear on the:

- A. existence of a set of functions and their specified properties
- B. ability of the software to be transferred from one environment to another
- C. capability of software to maintain its level of performance under stated conditions
- D. relationship between the performance of the software and the amount of resources used

Answer: A

Explanation:

Functionality is the set of attributes that bears on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs. Choice B refers to portability, choice C refers to reliability and choice D refers to efficiency.

NEW QUESTION 405

- (Topic 4)

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

- A. facilitates user involvement
- B. allows early testing of technical features
- C. facilitates conversion to the new system
- D. shortens the development time frame

Answer: D

Explanation:

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

NEW QUESTION 409

- (Topic 4)

An IS auditor reviewing a proposed application software acquisition should ensure that the:

- A. operating system (OS) being used is compatible with the existing hardware platform
- B. planned OS updates have been scheduled to minimize negative impacts on company needs
- C. OS has the latest versions and updates
- D. products are compatible with the current or planned OS

Answer: D

Explanation:

Choices A, B and C are incorrect because none of them are related to the area being audited. In reviewing the proposed application the auditor should ensure that the products to be purchased are compatible with the current or planned OS. Regarding choice A, if the OS is currently being used, it is compatible with the existing hardware platform, because if it is not it would not operate properly. In choice B, the planned OS updates should be scheduled to minimize negative impacts on the organization. For choice C, the installed OS should be equipped with the most recent versions and updates (with sufficient history and stability).

NEW QUESTION 414

- (Topic 4)

Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?

- A. A sufficient quantity of data for each test case
- B. Data representing conditions that are expected in actual processing
- C. Completing the test on schedule
- D. A random sample of actual data

Answer: B

Explanation:

Selecting the right kind of data is key in testing a computer system. The data should not only include valid and invalid data but should be representative of actual processing; quality is more important than quantity. It is more important to have adequate test data than to complete the testing on schedule. It is unlikely that a random sample of actual data would cover all test conditions and provide a reasonable representation of actual data.

NEW QUESTION 416

- (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 applications
- 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 420

- (Topic 4)

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

- A. conceptual design specification
- B. vendor contract
- C. error report

D. program change request

Answer: C

Explanation:

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

NEW QUESTION 423

- (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 425

- (Topic 4)

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

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

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 427

- (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 430

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 434

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 437

- (Topic 4)

An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?

- A. Pilot
- B. Parallel
- C. Direct cutover
- D. Phased

Answer: C

Explanation:

Direct cutover implies switching to the new system immediately, usually without the ability to revert to the old system in the event of problems. All other alternatives are done gradually and thus provide greater recoverability and are therefore less risky.

NEW QUESTION 438

- (Topic 4)

The reason a certification and accreditation process is performed on critical systems is to ensure that:

- A. security compliance has been technically evaluated
- B. data have been encrypted and are ready to be stored
- C. the systems have been tested to run on different platforms
- D. the systems have followed the phases of a waterfall model

Answer: A

Explanation:

Certified and accredited systems are systems that have had their security compliance technically evaluated for running on a specific production server. Choice B is incorrect because not all data of certified systems are encrypted. Choice C is incorrect because certified systems are evaluated to run in a specific environment. A waterfall model is a software development methodology and not a reason for performing a certification and accrediting process.

NEW QUESTION 440

- (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 compliance
- C. Ensure that only authorized personnel can update the databases
- D. Establish controls to handle concurrent access problems

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 a detective 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 443

- (Topic 4)

An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

- A. Log all table update transaction
- B. implement before-and-after image reportin
- C. Use tracing and taggin
- D. implement integrity constraints in the databas

Answer: D

Explanation:

Implementing integrity constraints in the database is a preventive control, because data is checked against predefined tables or rules preventing any undefined data from being entered. Logging all table update transactions and implementing before-and-after image reporting are detective controls that would not avoid the situation. Tracing and tagging are used to test application systems and controls and could not prevent out-of-range data.

NEW QUESTION 447

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 450

- (Topic 4)

An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:

- A. EDI trading partner agreement
- B. physical controls for terminal
- C. authentication techniques for sending and receiving message
- D. program change control procedure

Answer: C

Explanation:

Authentication techniques for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

NEW QUESTION 451

- (Topic 4)

When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:

- A. not be concerned since there may be other compensating controls to mitigate the risk
- B. ensure that overrides are automatically logged and subject to review
- C. verify whether all such overrides are referred to senior management for approval
- D. recommend that overrides not be permitted

Answer: B

Explanation:

If input procedures allow overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log. An IS auditor should not assume that compensating controls exist. As long as the overrides are policy-compliant, there is no need for senior management approval or a blanket prohibition.

NEW QUESTION 455

- (Topic 4)

An IS auditor reviewing an accounts payable system discovers that audit logs are not being reviewed. When this issue is raised with management the response is that additional controls are not necessary because effective system access controls are in place. The BEST response the auditor can make is to:

- A. review the integrity of system access control
- B. accept management's statement that effective access controls are in place

- C. stress the importance of having a system control framework in plac
- D. review the background checks of the accounts payable staf

Answer: C

Explanation:

Experience has demonstrated that reliance purely on preventative controls is dangerous. Preventative controls may not prove to be as strong as anticipated or their effectiveness can deteriorate over time. Evaluating the cost of controls versus the quantum of risk is a valid management concern. However, in a high-risk system a comprehensive control framework is needed, intelligent design should permit additional detective and corrective controls to be established that don't have high ongoing costs, e.g., automated interrogation of logs to highlight suspicious individual transactions or data patterns. Effective access controls are, in themselves, a positive but, for reasons outlined above, may not sufficiently compensate for other control weaknesses. In this situation the IS auditor needs to be proactive. The IS auditor has a fundamental obligation to point out control weaknesses that give rise to unacceptable risks to the organization and work with management to have these corrected. Reviewing background checks on accounts payable staff does not provide evidence that fraud will not occur.

NEW QUESTION 459

- (Topic 5)

The PRIMARY objective of service-level management (SLM) is to:

- A. define, agree, record and manage the required levels of servic
- B. ensure that services are managed to deliver the highest achievable level of availabilit
- C. keep the costs associated with any service at a minimu
- D. monitor and report any legal noncompliance to business managemen

Answer: A

Explanation:

The objective of service-level management (SLM) is to negotiate, document and manage (i.e., provide and monitor) the services in the manner in which the customer requires those services. This does not necessarily ensure that services are delivered at the highest achievable level of availability (e.g., redundancy and clustering). Although maximizing availability might be necessary for some critical services, it cannot be applied as a general rule of thumb. SLM cannot ensure that costs for all services will be kept at a low or minimum level, since costs associated with a service will directly reflect the customer's requirements. Monitoring and reporting legal noncompliance is not a part of SLM.

NEW QUESTION 461

- (Topic 5)

Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

- A. The use of diskless workstations
- B. Periodic checking of hard drives
- C. The use of current antivirus software
- D. Policies that result in instant dismissal if violated

Answer: B

Explanation:

The periodic checking of hard drives would be the most effective method of identifying illegal software packages loaded to the network. Antivirus software will not necessarily identify illegal software, unless the software contains a virus. Diskless workstations act as a preventive control and are not effective, since users could still download software from other than diskless workstations. Policies lay out the rules about loading the software, but will not detect the actual occurrence.

NEW QUESTION 463

- (Topic 5)

Applying a retention date on a file will ensure that:

- A. data cannot be read until the date is se
- B. data will not be deleted before that dat
- C. backup copies are not retained after that dat
- D. datasets having the same name are differentiate

Answer: B

Explanation:

A retention date will ensure that a file cannot be overwritten before that date has passed. The retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and therefore may be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

NEW QUESTION 466

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

CISA Practice Exam Features:

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