



Isaca

Exam Questions CISA

Isaca 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)

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

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

Answer: A

Explanation:

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

NEW QUESTION 3

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 4

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 5

- (Topic 1)

Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

- A. A neural network
- B. Database management software
- C. Management information systems
- D. Computer assisted audit techniques

Answer: A

Explanation:

A neural network will monitor and learn patterns, reporting exceptions for investigation.

NEW QUESTION 6

- (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 7

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 8

- (Topic 1)

As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

- A. The same value
- B. Greater value
- C. Lesser value
- D. Prior audit reports are not relevant

Answer: C

Explanation:

Prior audit reports are considered of lesser value to an IS auditor attempting to gain an understanding of an organization's IT process than evidence directly collected.

NEW QUESTION 9

- (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 10

- (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 10

- (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 13

- (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 16

- (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 17

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 21

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 24

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 28

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 29

- (Topic 1)

What increases encryption overhead and cost the most?

- A. A long symmetric encryption key
- B. A long asymmetric encryption key
- C. A long Advance Encryption Standard (AES) key
- D. A long Data Encryption Standard (DES) key

Answer: B

Explanation:

A long asymmetric encryption key (public key encryption) increases encryption overhead and cost. All other answers are single shared symmetric keys.

NEW QUESTION 34

- (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 39

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 41

- (Topic 1)

Which of the following provides the strongest authentication for physical access control?

- A. Sign-in logs
- B. Dynamic passwords
- C. Key verification
- D. Biometrics

Answer: D

Explanation:

Biometrics can be used to provide excellent physical access control.

NEW QUESTION 46

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 50

- (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 54

- (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 59

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 61

- (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 66

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 68

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 72

- (Topic 1)

Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs. True or false?

- A. True
- B. False

Answer: B

Explanation:

Function point analysis (FPA) provides an estimate of the size of an information system based on the number and complexity of a system's inputs, outputs, and files.

NEW QUESTION 75

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 77

- (Topic 1)

Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

- A. True
- B. False

Answer: A

Explanation:

Network environments often add to the complexity of program-to-program communication, making application systems implementation and maintenance more difficult.

NEW QUESTION 82

- (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 85

- (Topic 1)

An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

- A. True
- B. False

Answer: B

Explanation:

An intentional or unintentional disclosure of a password is not likely to be evident within control logs.

NEW QUESTION 87

- (Topic 1)

When are benchmarking partners identified within the benchmarking process?

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

Answer: C

Explanation:

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

NEW QUESTION 90

- (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 93

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 95

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 99

- (Topic 1)

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

- A. True
- B. False

Answer: B

Explanation:

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

NEW QUESTION 103

- (Topic 1)

What process allows IS management to determine whether the activities of the organization differ from the planned or expected levels? Choose the BEST answer.

- A. Business impact assessment
- B. Risk assessment
- C. IS assessment methods
- D. Key performance indicators (KPIs)

Answer: C

Explanation:

IS assessment methods allow IS management to determine whether the activities of the organization differ from the planned or expected levels.

NEW QUESTION 104

- (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 105

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 107

- (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 112

- (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 115

- (Topic 1)

What can be used to gather evidence of network attacks?

- A. Access control lists (ACL)
- B. Intrusion-detection systems (IDS)
- C. Syslog reporting
- D. Antivirus programs

Answer: B

Explanation:

Intrusion-detection systems (IDS) are used to gather evidence of network attacks.

NEW QUESTION 119

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 120

- (Topic 1)

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

- A. False
- B. True

Answer: B

Explanation:

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

NEW QUESTION 121

- (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 122

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 127

- (Topic 1)

What should IS auditors always check when auditing password files?

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

Answer: B

Explanation:

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

NEW QUESTION 129

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 134

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 138

- (Topic 1)

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 142

- (Topic 1)

Off-site data storage should be kept synchronized when preparing for recovery of time-sensitive data such as that resulting from which of the following? Choose the BEST answer.

- A. Financial reporting
- B. Sales reporting
- C. Inventory reporting
- D. Transaction processing

Answer: D

Explanation:

Off-site data storage should be kept synchronized when preparing for the recovery of timesensitive data such as that resulting from transaction processing.

NEW QUESTION 147

- (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 150

- (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 151

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 156

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 161

- (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 165

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 170

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 173

- (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 174

- (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 176

- (Topic 2)

Which of the following is a substantive test?

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

Answer: C

Explanation:

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

NEW QUESTION 180

- (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 181

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 184

- (Topic 2)

In planning an audit, the MOST critical step is the identification of the:

- A. areas of high risk
- B. skill sets of the audit staff
- C. test steps in the audit
- D. time allotted for the audit

Answer: A

Explanation:

When designing an audit plan, it is important to identify the areas of highest risk to determine the areas to be audited. The skill sets of the audit staff should have been considered before deciding and selecting the audit. Test steps for the audit are not as critical as identifying the areas of risk, and the time allotted for an audit is determined by the areas to be audited, which are primarily selected based on the identification of risks.

NEW QUESTION 189

- (Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 191

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 193

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 198

- (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 201

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 203

- (Topic 2)

Which of the following is an advantage of an integrated test facility (ITF)?

- A. It uses actual master files or dummies and the IS auditor does not have to review the source of the transactions
- B. Periodic testing does not require separate test processes
- C. It validates application systems and tests the ongoing operation of the system
- D. The need to prepare test data is eliminated

Answer: B

Explanation:

An integrated test facility creates a fictitious entity in the database to process test transactions simultaneously with live input. Its advantage is that periodic testing does not require separate test processes. However, careful planning is necessary, and test data must be isolated from production data.

NEW QUESTION 207

- (Topic 2)

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

- A. efficiency of the application in meeting the business processes

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

Answer: B

Explanation:

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

NEW QUESTION 210

- (Topic 2)

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

- A. determining whether bar code readers are installe
- B. determining whether the movement of tapes is authorize
- C. conducting a physical count of the tape inventor
- D. checking if receipts and issues of tapes are accurately recorde

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 215

- (Topic 2)

An IS auditor issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommends a vendor product to address this vulnerability. The IS auditor has failed to exercise:

- A. professional independence
- B. organizational independenc
- C. technical competenc
- D. professional competenc

Answer: A

Explanation:

When an IS auditor recommends a specific vendor, they compromise professional independence. Organizational independence has no relevance to the content of an audit report and should be considered at the time of accepting the engagement. Technical and professional competence is not relevant to the requirement of independence.

NEW QUESTION 217

- (Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 220

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 223

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 228

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 233

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 236

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 239

- (Topic 3)

Effective IT governance will ensure that the IT plan is consistent with the organization's:

- A. business pla
- B. audit pla
- C. security pla
- D. investment pla

Answer:

A

Explanation:

To govern IT effectively, IT and business should be moving in the same direction, requiring that the IT plans are aligned with an organization's business plans. The audit and investment plans are not part of the IT plan, while the security plan should be at a corporate level.

NEW QUESTION 241

- (Topic 3)

IT governance is PRIMARILY the responsibility of the:

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

Answer: B

Explanation:

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

NEW QUESTION 244

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 248

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 249

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 251

- (Topic 3)

An IS auditor should be concerned when a telecommunication analyst:

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

Answer: A

Explanation:

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

NEW QUESTION 253

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 257

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 262

- (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 266

- (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 268

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 272

- (Topic 3)

When reviewing an organization's strategic IT plan an IS auditor should expect to find:

- A. an assessment of the fit of the organization's application portfolio with business objective
- B. actions to reduce hardware procurement cos
- C. a listing of approved suppliers of IT contract resource
- D. a description of the technical architecture for the organization's network perimeter securit

Answer: A

Explanation:

An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions. Further assessment can then be made of how well the overall IT organization, encompassing applications, infrastructure, services, management processes, etc., can support the business objectives. Operational efficiency initiatives belong to tactical planning, not strategic planning. The purpose of an IT strategic plan is to set out how IT will be used to achieve or support an organization's business objectives. A listing of approved suppliers of IT contract resources is a tactical rather than a strategic concern. An IT strategic plan would not normally include detail of a specific technical architecture.

NEW QUESTION 274

- (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 276

- (Topic 3)

Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

- A. Assimilation of the framework and intent of a written security policy by all appropriate parties
- B. Management support and approval for the implementation and maintenance of a security policy
- C. Enforcement of security rules by providing punitive actions for any violation of security rules
- D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Answer: A

Explanation:

Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and

provision for punitive actions for violation of security rules, is also required, along with the user's education on the importance of security.

NEW QUESTION 281

- (Topic 3)

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

- A. recover
- B. retention
- C. rebuilding
- D. reuse

Answer: B

Explanation:

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

NEW QUESTION 284

- (Topic 3)

Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?

- A. Define a balanced scorecard (BSC) for measuring performance
- B. Consider user satisfaction in the key performance indicators (KPIs)
- C. Select projects according to business benefits and risks
- D. Modify the yearly process of defining the project portfolio

Answer: C

Explanation:

Prioritization of projects on the basis of their expected benefit(s) to business, and the related risks, is the best measure for achieving alignment of the project portfolio to an organization's strategic priorities. Modifying the yearly process of the projects portfolio definition might improve the situation, but only if the portfolio definition process is currently not tied to the definition of corporate strategies; however, this is unlikely since the difficulties are in maintaining the alignment, and not in setting it up initially. Measures such as balanced scorecard (BSC) and key performance indicators (KPIs) are helpful, but they do not guarantee that the projects are aligned with business strategy.

NEW QUESTION 288

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 292

- (Topic 3)

After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

- A. Project management and progress reporting is combined in a project management office which is driven by external consultant
- B. The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach
- C. The resources of each of the organizations are inefficiently allocated while they are being familiarized with the other company's legacy system
- D. The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training need

Answer: B

Explanation:

The efforts should be consolidated to ensure alignment with the overall strategy of the postmerger organization. If resource allocation is not centralized, the separate projects are at risk of overestimating the availability of key knowledge resources for the in-house developed legacy applications. In postmerger integration programs, it is common to form project management offices to ensure standardized and comparable information levels in the planning and reporting structures, and to centralized dependencies of project deliverables or resources. The experience of external consultants can be valuable since project management practices do not require in-depth knowledge of the legacy systems. This can free up resources for functional tasks. It is a good idea to first get familiar with the old systems, to understand what needs to be done in a migration and to evaluate the implications of technical decisions. In most cases, mergers result in application changes and thus in training needs as organizations and processes change to leverage the intended synergy effects of the merger.

NEW QUESTION 297

- (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 302

- (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 307

- (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 309

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 310

- (Topic 3)

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

- A. vulnerabilities
- B. threats
- C. probabilities
- D. impacts

Answer: A

Explanation:

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

NEW QUESTION 315

- (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 316

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 320

- (Topic 4)

The most common reason for the failure of information systems to meet the needs of users is that:

- A. user needs are constantly changing
- B. the growth of user requirements was forecast inaccurately
- C. the hardware system limits the number of concurrent users
- D. user participation in defining the system's requirements was inadequate

Answer: D

Explanation:

Lack of adequate user involvement, especially in the system's requirements phase, will usually result in a system that does not fully or adequately address the needs of the user. Only users can define what their needs are, and therefore what the system should accomplish.

NEW QUESTION 322

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 323

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 324

- (Topic 4)

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 analyze
- B. resources needed throughout the project have been determine
- C. project deliverables have been identifie
- D. a contract for external parties involved in the project has been complete

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 327

- (Topic 4)

An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start impacting the project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

- A. stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plan
- B. accept the project manager's position as the project manager is accountable for the outcome of the projec
- C. offer to work with the risk manager when one is appointe
- D. inform the project manager that the IS auditor will conduct a review of the risks at the completion of the requirements definition phase of the projec

Answer: A

Explanation:

The majority of project risks can typically be identified before a project begins, allowing mitigation/avoidance plans to be put in place to deal with these risks. A project should have a clear link back to corporate strategy and tactical plans to support this strategy. The process of setting corporate strategy, setting objectives and developing tactical plans should include the consideration of risks. Appointing a risk manager is a good practice but waiting until the project has been impacted by risks is misguided. Risk management needs to be forward looking; allowing risks to evolve into issues that adversely impact the project represents a failure of risk management. With or without a risk manager, persons within and outside of the project team need to be consulted and encouraged to comment when they believe new risks have emerged or risk priorities have changed. The IS auditor has an obligation to the project sponsor and the organization to advise on appropriate project management practices. Waiting for the possible appointment of a risk manager represents an unnecessary and dangerous delay to implementing risk management.

NEW QUESTION 329

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 334

- (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 336

- (Topic 4)

An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. Of the following, who is PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

- A. Project sponsor
- B. System development project team (SDPT)
- C. Project steering committee
- D. User project team (UPT)

Answer: C

Explanation:

A project steering committee that provides an overall direction for the enterprise resource planning (ERP) implementation project is responsible for reviewing the project's progress to ensure that it will deliver the expected results. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support. The sponsor provides funding for the project and works closely with the project manager to define the critical success factors or metrics for the project. The project sponsor is not responsible for reviewing the progress of the project. A system development project team (SDPT) completes the assigned tasks, works according to the instructions of the project manager and communicates with the user project team. The SDPT is not responsible for reviewing the progress of the project. A user project team (UPT) completes the assigned tasks, communicates effectively with the system development team and works according to the advice of the project manager. A UPT is not responsible for reviewing the progress of the project.

NEW QUESTION 337

- (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 progress 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 340

- (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 341

- (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 preparation
- B. in transit to the computer
- C. between related computer runs
- D. during the return of the data to the user department

Answer: A

Explanation:

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

NEW QUESTION 344

- (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 348

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 349

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 351

- (Topic 4)

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

- A. System testing
- B. Acceptance testing

- C. Integration testing
- D. Unit testing

Answer: B

Explanation:

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

NEW QUESTION 352

- (Topic 4)

Which of the following is the most important element in the design of a data warehouse?

- A. Quality of the metadata
- B. Speed of the transactions
- C. Volatility of the data
- D. Vulnerability of the system

Answer: A

Explanation:

Quality of the metadata is the most important element in the design of a data warehouse. A data warehouse is a copy of transaction data specifically structured for query and analysis. Metadata aim to provide a table of contents to the information stored in the data warehouse. Companies that have built warehouses believe that metadata are the most important component of the warehouse.

NEW QUESTION 355

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 359

- (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 362

- (Topic 4)

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

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

Answer: B

Explanation:

It would be most important to complete the user acceptance testing to ensure that the system to be implemented is working correctly. The completion of the user

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

NEW QUESTION 363

- (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 need
- C. OS has the latest versions and update
- 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 365

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 367

- (Topic 4)

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

- A. test data covering critical application
- B. detailed test plan
- C. quality assurance test specification
- D. user acceptance testing specification

Answer: D

Explanation:

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

NEW QUESTION 372

- (Topic 4)

Which of the following is an advantage of the top-down approach to software testing?

- A. Interface errors are identified early
- B. Testing can be started before all programs are complete
- C. it is more effective than other testing approaches
- D. Errors in critical modules are detected sooner

Answer: A

Explanation:

The advantage of the top-down approach is that tests of major functions are conducted early, thus enabling the detection of interface errors sooner. The most effective testing approach is dependent on the environment being tested. Choices B and D are advantages of the bottom-up approach to system testing.

NEW QUESTION 375

- (Topic 4)

The specific advantage of white box testing is that it:

- A. verifies a program can operate successfully with other parts of the system
- B. ensures a program's functional operating effectiveness without regard to the internal program structure

- C. determines procedural accuracy or conditions of a program's specific logic path
- D. examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system

Answer: C

Explanation:

White box testing assesses the effectiveness of software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's logic paths. Verifying the program can operate successfully with other parts of the system is sociability testing. Testing the program's functionality without knowledge of internal structures is black box testing. Controlled testing of programs in a semi-debugged environment, either heavily controlled step-by-step or via monitoring in virtual machines, is sand box testing.

NEW QUESTION 377

- (Topic 4)

Which of the following is an implementation risk within the process of decision support systems?

- A. Management control
- B. Semistructured dimensions
- C. inability to specify purpose and usage patterns
- D. Changes in decision processes

Answer: C

Explanation:

The inability to specify purpose and usage patterns is a risk that developers need to anticipate while implementing a decision support system (DSS). Choices A, B and D are not risks, but characteristics of a DSS.

NEW QUESTION 379

- (Topic 4)

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

- A. security compliance has been technically evaluate
- B. data have been encrypted and are ready to be store
- C. the systems have been tested to run on different platform
- D. the systems have followed the phases of a waterfall mode

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 382

- (Topic 4)

Responsibility and reporting lines cannot always be established when auditing automated systems since:

- A. diversified control makes ownership irrelevant
- B. staff traditionally changes jobs with greater frequenc
- C. ownership is difficult to establish where resources are share
- D. duties change frequently in the rapid development of technolog

Answer: C

Explanation:

Because of the diversified nature of both data and application systems, the actual owner of data and applications may be hard to establish.

NEW QUESTION 386

- (Topic 4)

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

- A. Develop a baseline and monitor system usag
- B. Define alternate processing procedure
- C. Prepare the maintenance manua
- D. implement the changes users have suggeste

Answer: A

Explanation:

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

NEW QUESTION 387

- (Topic 4)

Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would MOST likely focus on a review of:

- A. pre-BPR process flowchart
- B. post-BPR process flowchart
- C. BPR project plan
- D. continuous improvement and monitoring plan

Answer: B

Explanation:

An IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process. Choice A is incorrect because an IS auditor must review the process as it is today, not as it was in the past. Choices C and D are incorrect because they are steps within a BPR project.

NEW QUESTION 391

- (Topic 4)

Which of the following is the MOST critical and contributes the greatest to the quality of data in a data warehouse?

- A. Accuracy of the source data
- B. Credibility of the data source
- C. Accuracy of the extraction process
- D. Accuracy of the data transformation

Answer: A

Explanation:

Accuracy of source data is a prerequisite for the quality of the data in a data warehouse. Credibility of the data source, accurate extraction processes and accurate transformation routines are all important, but would not change inaccurate data into quality (accurate) data.

NEW QUESTION 394

- (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 396

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 398

- (Topic 4)

The GREATEST advantage of using web services for the exchange of information between two systems is:

- A. secure communication
- B. improved performance
- C. efficient interfacing
- D. enhanced documentation

Answer: C

Explanation:

Web services facilitate the exchange of information between two systems, regardless of the operating system or programming language used. Communication is not necessarily securer or faster, and there is no documentation benefit in using web services.

NEW QUESTION 403

- (Topic 4)

When reviewing an organization's approved software product list, which of the following is the MOST important thing to verify?

- A. The risks associated with the use of the products are periodically assessed
- B. The latest version of software is listed for each product
- C. Due to licensing issues the list does not contain open source software
- D. After hours support is offered

Answer: A

Explanation:

Since the business conditions surrounding vendors may change, it is important for an organization to conduct periodic risk assessments of the vendor software list. This might be best incorporated into the IT risk management process. Choices B, C and D are possible considerations but would not be the most important.

NEW QUESTION 404

- (Topic 4)

An IS auditor performing an application maintenance audit would review the log of program changes for the:

- A. authorization of program change
- B. creation date of a current object modul
- C. number of program changes actually mad
- D. creation date of a current source progra

Answer: A

Explanation:

The manual log will most likely contain information on authorized changes to a program. Deliberate, unauthorized changes will not be documented by the responsible party. An automated log, found usually in library management products, and not a changelog would most likely contain date information for the source and executable modules.

NEW QUESTION 409

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 410

- (Topic 5)

An organization has outsourced its help desk. Which of the following indicators would be the best to include in the SLA?

- A. Overall number of users supported
- B. Percentage of incidents solved in the first call
- C. Number of incidents reported to the help desk
- D. Number of agents answering the phones

Answer: B

Explanation:

Since it is about service level (performance) indicators, the percentage of incidents solved on the first call is the only option that is relevant. Choices A, C and D are not quality measures of the help desk service.

NEW QUESTION 414

- (Topic 5)

Which of the following should be of PRIMARY concern to an IS auditor reviewing the management of external IT service providers?

- A. Minimizing costs for the services provided
- B. Prohibiting the provider from subcontracting services
- C. Evaluating the process for transferring knowledge to the IT department
- D. Determining if the services were provided as contracted

Answer: D

Explanation:

From an IS auditor's perspective, the primary objective of auditing the management of service providers should be to determine if the services that were requested were provided in a way that is acceptable, seamless and in line with contractual agreements. Minimizing costs, if applicable and achievable (depending on the customer's need) is traditionally not part of an IS auditor's job. This would normally be done by a line management function within the IT department. Furthermore, during an audit, it is too late to minimize the costs for existing provider arrangements. Subcontracting providers could be a concern, but it would not be the primary concern. Transferring knowledge to the internal IT department might be desirable under certain circumstances, but should not be the primary concern of an IS auditor when auditing IT service providers and the management thereof.

NEW QUESTION 417

- (Topic 5)

IT best practices for the availability and continuity of IT services should:

- A. minimize costs associated with disaster-resilient component
- B. provide for sufficient capacity to meet the agreed upon demands of the business
- C. provide reasonable assurance that agreed upon obligations to customers can be met
- D. produce timely performance metric report

Answer: C

Explanation:

It is important that negotiated and agreed commitments (i.e., service level agreements [SLAs]) can be fulfilled all the time. If this were not achievable, IT should not have agreed to these requirements, as entering into such a commitment would be misleading to the business. 'All the time' in this context directly relates to the 'agreed obligations' and does not imply that a service has to be available 100 percent of the time. Costs are a result of availability and service continuity management and may only be partially controllable. These costs directly reflect the agreed upon obligations. Capacity management is a necessary, but not sufficient, condition of availability. Despite the possibility that a lack of capacity may result in an availability issue, providing the capacity necessary for seamless operations of services would be done within capacity management, and not within availability management. Generating reports might be a task of availability and service continuity management, but that is true for many other areas of interest as well (e.g., incident, problem, capacity and change management).

NEW QUESTION 419

- (Topic 5)

Applying a retention date on a file will ensure that:

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

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 424

- (Topic 5)

The BEST way to minimize the risk of communication failures in an e-commerce environment would be to use:

- A. compression software to minimize transmission duration
- B. functional or message acknowledgment
- C. a packet-filtering firewall to reroute messages
- D. leased asynchronous transfer mode line

Answer: D

Explanation:

Leased asynchronous transfer mode lines are a way to avoid using public and shared infrastructures from the carrier or Internet service provider that have a greater number of communication failures. Choice A, compression software, is a valid way to reduce the problem, but is not as good as leased asynchronous transfer mode lines. Choice B is a control based on higher protocol layers and helps if communication lines are introducing noise, but not if a link is down. Choice C, a packet-filtering firewall, does not reroute messages.

NEW QUESTION 429

- (Topic 5)

The objective of concurrency control in a database system is to:

- A. restrict updating of the database to authorized user
- B. prevent integrity problems when two processes attempt to update the same data at the same time
- C. prevent inadvertent or unauthorized disclosure of data in the database
- D. ensure the accuracy, completeness and consistency of data

Answer: B

Explanation:

Concurrency controls prevent data integrity problems, which can arise when two update processes access the same data item at the same time. Access controls restrict updating of the database to authorized users, and controls such as passwords prevent the inadvertent or unauthorized disclosure of data from the database. Quality controls, such as edits, ensure the accuracy, completeness and consistency of data maintained in the database.

NEW QUESTION 434

- (Topic 5)

Which of the following database controls would ensure that the integrity of transactions is maintained in an online transaction processing system's database?

- A. Authentication controls
- B. Data normalization controls
- C. Read/write access log controls
- D. Commitment and rollback controls

Answer: D

Explanation:

Commitment and rollback controls are directly relevant to integrity. These controls ensure that database operations that form a logical transaction unit will complete in its entirety or not at all; i.e., if, for some reason, a transaction cannot be fully completed, then incomplete inserts/updates/deletes are rolled back so that the database returns to its pretransaction state. All other choices would not address transaction integrity.

NEW QUESTION 436

- (Topic 5)

Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?

- A. Parity check
- B. Echo check
- C. Block sum check
- D. Cyclic redundancy check

Answer: D

Explanation:

The cyclic redundancy check (CRC) can check for a block of transmitted data. The workstations generate the CRC and transmit it with the data. The receiving workstation computes a CRC and compares it to the transmitted CRC. If both of them are equal, then the block is assumed error free, in this case (such as in parity error or echo check), multiple errors can be detected. In general, CRC can detect all single-bit and bubble-bit errors. Parity check (known as vertical redundancy check) also involves adding a bit (known as the parity bit) to each character during transmission. In this case, where there is a presence of bursts of errors (i.e., impulsive noise during high transmission rates), it has a reliability of approximately 50 percent. In higher transmission rates, this limitation is significant. Echo checks detect line errors by retransmitting data to the sending device for comparison with the original transmission.

NEW QUESTION 439

- (Topic 5)

Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?

- A. Assess the impact of patches prior to installation
- B. Ask the vendors for a new software version with all fixes included
- C. Install the security patch immediately
- D. Decline to deal with these vendors in the future

Answer: A

Explanation:

The effect of installing the patch should be immediately evaluated and installation should occur based on the results of the evaluation. To install the patch without knowing what it might affect could easily cause problems. New software versions with all fixes included are not always available and a full installation could be time consuming. Declining to deal with vendors does not take care of the flaw.

NEW QUESTION 441

- (Topic 5)

Change management procedures are established by IS management to:

- A. control the movement of applications from the test environment to the production environment
- B. control the interruption of business operations from lack of attention to unresolved problems
- C. ensure the uninterrupted operation of the business in the event of a disaster
- D. verify that system changes are properly documented

Answer: A

Explanation:

Change management procedures are established by IS management to control the movement of applications from the test environment to the production environment. Problem escalation procedures control the interruption of business operations from lack of attention to unresolved problems, and quality assurance procedures verify that system changes are authorized and tested.

NEW QUESTION 445

- (Topic 5)

An IS auditor should recommend the use of library control software to provide reasonable assurance that:

- A. program changes have been authorize
- B. only thoroughly tested programs are release
- C. modified programs are automatically moved to productio
- D. source and executable code integrity is maintaine

Answer: A

Explanation:

Library control software should be used to separate test from production libraries in mainframe and/or client server environments. The main objective of library control software is to provide assurance that program changes have been authorized. Library control software is concerned with authorized program changes and would not automatically move modified programs into production and cannot determine whether programs have been thoroughly tested. Library control software provides reasonable assurance that the source code and executable code are matched at the time a source code is moved to production. However, subsequent events such as a hardware failure can result in a lack of consistency between source and executable code.

NEW QUESTION 449

- (Topic 5)

When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

- A. allow changes, which will be completed using after-the-fact follow-u
- B. allow undocumented changes directly to the production librar
- C. do not allow any emergency change
- D. allow programmers permanent access to production program

Answer: A

Explanation:

There may be situations where emergency fixes are required to resolve system problems. This involves the use of special logon IDs that grant programmers temporary access to production programs during emergency situations. Emergency changes should be completed using after-the-fact follow-up procedures, which ensure that normal procedures are retroactively applied; otherwise, production may be impacted. Changes made in this fashion should be held in an emergency library from where they can be moved to the production library, following the normal change management process. Programmers should not directly alter the production library nor should they be allowed permanent access to production programs.

NEW QUESTION 453

- (Topic 5)

An IS auditor discovers that developers have operator access to the command line of a production environment operating system. Which of the following controls would BEST mitigate the risk of undetected and unauthorized program changes to the production environment?

- A. Commands typed on the command line are logged
- B. Hash keys are calculated periodically for programs and matched against hash keys calculated for the most recent authorized versions of the programs
- C. Access to the operating system command line is granted through an access restriction tool with preapproved rights
- D. Software development tools and compilers have been removed from the production environment

Answer: B

Explanation:

The matching of hash keys over time would allow detection of changes to files. Choice A is incorrect because having a log is not a control, reviewing the log is a control. Choice C is incorrect because the access was already granted-it does not matter how. Choice D is wrong because files can be copied to and from the production environment.

NEW QUESTION 454

- (Topic 5)

Which of the following processes should an IS auditor recommend to assist in the recording of baselines for software releases?

- A. Change management
- B. Backup and recovery
- C. incident management
- D. Configuration management

Answer: D

Explanation:

The configuration management process may include automated tools that will provide an automated recording of software release baselines. Should the new

release fail, the baseline will provide a point to which to return. The other choices do not provide the processes necessary for establishing software release baselines and are not related to software release baselines.

NEW QUESTION 455

- (Topic 5)

The PRIMARY objective of performing a postincident review is that it presents an opportunity to:

- A. improve internal control procedure
- B. harden the network to industry best practice
- C. highlight the importance of incident response management to management
- D. improve employee awareness of the incident response process

Answer: A

Explanation:

A postincident review examines both the cause and response to an incident. The lessons learned from the review can be used to improve internal controls. Understanding the purpose and structure of postincident reviews and follow-up procedures enable the information security manager to continuously improve the security program. Improving the incident response plan based on the incident review is an internal (corrective) control. The network may already be hardened to industry best practices. Additionally, the network may not be the source of the incident. The primary objective is to improve internal control procedures, not to highlight the importance of incident response management (IRM), and an incident response (IR) review does not improve employee awareness.

NEW QUESTION 458

- (Topic 5)

The MAIN criterion for determining the severity level of a service disruption incident is:

- A. cost of recovery
- B. negative public opinion
- C. geographic location
- D. downtime

Answer: D

Explanation:

The longer the period of time a client cannot be serviced, the greater the severity of the incident. The cost of recovery could be minimal yet the service downtime could have a major impact. Negative public opinion is a symptom of an incident. Geographic location does not determine the severity of the incident.

NEW QUESTION 462

- (Topic 5)

Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

- A. Firewalls
- B. Routers
- C. Layer 2 switches
- D. VLANs

Answer: A

Explanation:

Firewall systems are the primary tool that enable an organization to prevent unauthorized access between networks. An organization may choose to deploy one or more systems that function as firewalls. Routers can filter packets based on parameters, such as source address, but are not primarily a security tool. Based on Media Access Control (MAC) addresses, layer 2 switches separate traffic in a port as different segments and without determining if it is authorized or unauthorized traffic. A virtual LAN (VLAN) is a functionality of some switches that allows them to switch the traffic between different ports as if they are in the same LAN. Nevertheless, they do not deal with authorized vs. unauthorized traffic.

NEW QUESTION 466

- (Topic 5)

An IS auditor is performing a network security review of a telecom company that provides Internet connection services to shopping malls for their wireless customers. The company uses Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned if a hacker:

- A. compromises the Wireless Application Protocol (WAP) gateway
- B. installs a sniffing program in front of the server
- C. steals a customer's PD
- D. listens to the wireless transmission

Answer: A

Explanation:

In a WAP gateway, the encrypted messages from customers must be decrypted to transmit over the Internet and vice versa. Therefore, if the gateway is compromised, all of the messages would be exposed. SSL protects the messages from sniffing on the Internet, limiting disclosure of the customer's information. WTLS provides authentication, privacy and integrity and prevents messages from eavesdropping.

NEW QUESTION 469

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The CISA Practice Test Here](#)