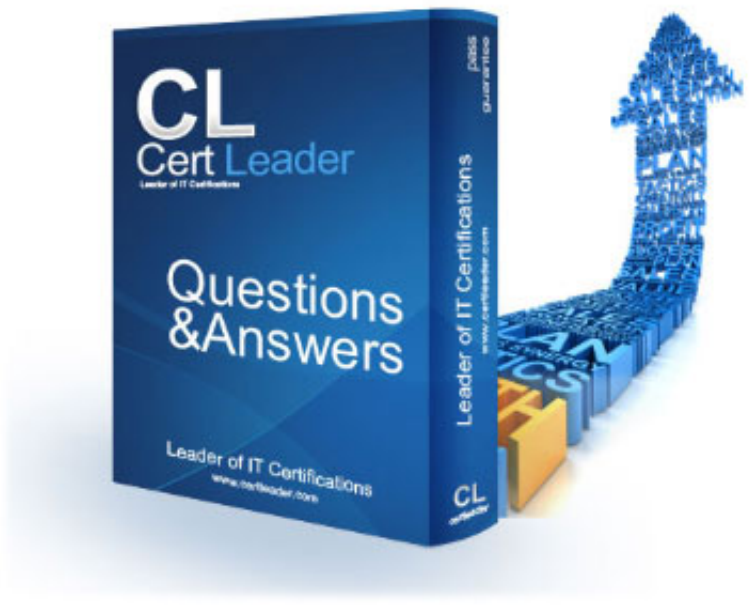
CISA Dumps

Isaca CISA

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



NEW QUESTION 1
IS management has decided to rewrite a legacycustomer relations system using fourth generation languages (4GLs). Which of the following risks is MOST often associated with system development using 4GLs?

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

Answer: D

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

NEW QUESTION 2
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 3
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 4
Which of the following is MOST likely to result from a business process reengineering (BPR) project?

A. An increased number of people using technology
B. Significant cost savings, through a reduction in the complexity of information technology
C. A weaker organizational structures and less accountability
D. Increased information protection (IP) risk will increase

Answer: A

Explanation:
A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern. Incorrect answers:
B. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this areA.
D. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

NEW QUESTION 5
Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

A. Router
B. Bridge
C. Repeater
D. Gateway

Answer: B

Explanation:
A bridge connects two separate networks to form a logical network (e.g., joining an ethernet and token network) and has the storage capacity to store frames and act as a storage and forward device. Bridges operate at the OSI data link layer by examining the media access control header of a data packet.

NEW QUESTION 6
Which of the following is a benefit of using callback devices?

A. Provide an audit trail
B. Can be used in a switchboard environment
C. Permit unlimited user mobility
D. Allow call forwarding

Answer: A

Explanation:
A callback feature hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches. Call forwarding (choice D) is a means of potentially bypassing callback control. By dialing through an authorized phone number from an unauthorized phone number, a perpetrator can gain computer access. This vulnerability can be controlled through callback systems that are available.

NEW QUESTION 7
A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

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

Answer: A

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

NEW QUESTION 8
Structured programming is BEST described as a technique that:

A. provides knowledge of program functions to other programmers via peer review
B. reduces the maintenance time of programs by the use of small-scale program module
C. makes the readable coding reflect as closely as possible the dynamic execution of the progra
D. controls the coding and testing of the high-level functions of the program in the development proces

Answer: B

Explanation:
A characteristic of structured programming is smaller, workable units. Structured programming has evolved because smaller, workable units are easier to maintain. Structured programming is a style of programming which restricts the kinds of control structures. This limitation is not crippling. Any program can be written with allowed control structures. Structured programming is sometimes referred to as go-to-less programming, since a go-to statement is not allowed. This is perhaps the most well known restriction of the style, since go-to statements were common at the time structured programming was becoming more popular. Statement labels also become unnecessary, except in languages where subroutines are identified by labels.

NEW QUESTION 9
An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

A. cold sit
B. warm sit
C. dial-up sit
D. duplicate processing facilit

Answer: A

Explanation:
A cold site is ready to receive equipment but does not offer any components at the site in advance of the need.

NEW QUESTION 10
A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

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

Answer: B

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

NEW QUESTION 10
In an EDI process, the device which transmits and receives electronic documents is the:

A. communications handle
B. EDI translato
C. application interfac
D. EDI interfac

Answer: A

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

NEW QUESTION 11
The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

A. testing stag
B. evaluation stag
C. maintenance stag
D. early stages of plannin

Answer: D

Explanation:
Company.com in the early stages of a BCP will incur the most significant level of program development effort, which will level out as the BCP moves into maintenance, testing and evaluation stages. It is during the planning stage that an IS auditor will play an important role in obtaining senior management's commitment to resources and assignment of BCP responsibilities.

NEW QUESTION 15
Which of the following network configuration options contains a direct link between any two host machines?

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

Answer: D

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

NEW QUESTION 19
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 22
Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

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

Answer: B

Explanation:
A compliance test determines if controls are operating as designed and are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned whether program library controls are working properly, the IS

auditor might select a sample of programs to determine if the source and object versions are the same. In other words, the broad objective of any compliance test is to provide auditors with reasonable assurance that a particular control on which the auditor plans to rely is operating as the auditor perceived it in the preliminary evaluation.

NEW QUESTION 24
A data administrator is responsible for:

A. maintaining database system softwar
B. defining data elements, data names and their relationshi
C. developing physical database structure
D. developing data dictionary system softwar

Answer: B

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

NEW QUESTION 27
An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

A. defining the conceptual schem
B. defining security and integrity check
C. liaising with users in developing data mode
D. mapping data model with the internal schem

Answer: D

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

NEW QUESTION 30
Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

A. Spool
B. Cluster controller
C. Protocol converter
D. Front end processor

Answer: D

Explanation:
A front-end processor is a hardware device that connects all communication lines to a central computer to relieve the central computer.

NEW QUESTION 32
The use of a GANTT chart can:

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

Answer: A

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

NEW QUESTION 34
Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

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

Answer: A

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

NEW QUESTION 35
Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

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

Answer: C

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

NEW QUESTION 37
A hardware control that helps to detect errors when data are communicated from one computer to another is known as a:

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

Answer: D

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

NEW QUESTION 39
For which of the following applications would rapid recovery be MOST crucial?

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

Answer: A

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

NEW QUESTION 44
The initial step in establishing an information security program is the:

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

Answer: C

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

NEW QUESTION 45
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 49
An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST costeffective test of the DRP?

A. Full operational test
B. Preparedness test
C. Paper test
D. Regression test

Answer: B

Explanation:
A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for the disaster recovery.

NEW QUESTION 51
The IS auditor learns that when equipment was brought into the data center by a vendor, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?

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

Answer: B

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

NEW QUESTION 52
Company.com has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

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

Answer: B

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

NEW QUESTION 57
In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

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

Answer: A

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

NEW QUESTION 59
Which of the following is a data validation edit and control?

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

Answer:

B

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

NEW QUESTION 63
A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

A. reasonableness chec
B. parity chec
C. redundancy chec
D. check digit

Answer: C

Explanation:
A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of datA.

NEW QUESTION 65
What is the primary objective of a control self-assessment (CSA) program?

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

Answer: A

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

NEW QUESTION 70
As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

A. The same valu
B. Greater valu
C. Lesser valu
D. Prior audit reports are not relevan

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 72
What is the PRIMARY purpose of audit trails?

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

Answer: C

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

NEW QUESTION 77
How does the process of systems auditing benefit from using a risk-based approach to audit planning?

A. Controls testing starts earlie
B. Auditing resources are allocated to the areas of highest concer
C. Auditing risk is reduce
D. Controls testing is more thoroug

Answer: B

Explanation: Allocation of auditing resources to the areas of highest concern is a benefit of a risk-based approach to audit planning.

NEW QUESTION 82
After an IS auditor has identified threats and potential impacts, the auditor should:

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

Answer: A

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

NEW QUESTION 83
What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

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

Answer: B

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

NEW QUESTION 85
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 86
Who is accountable for maintaining appropriate security measures over information assets?

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

Answer: A

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

NEW QUESTION 89
Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 92
What should an IS auditor do if he or she observes that project-approval procedures do not exist?

A. Advise senior management to invest in project-management training for the staff
B. Create project-approval procedures for future project implementations
C. Assign project leaders
D. Recommend to management that formal approval procedures be adopted and documented

Answer: D

Explanation: If an IS auditor observes that project-approval procedures do not exist, the IS auditor should recommend to management that formal approval procedures be adopted and documented.

NEW QUESTION 93

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

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

Answer: A

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

NEW QUESTION 95
Proper segregation of duties normally does not prohibit a LAN administrator from also having programming responsibilities. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 96
A core tenant of an IS strategy is that it must:

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

Answer: D

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

NEW QUESTION 101
Batch control reconciliation is a _____ (fill in the blank) control for mitigating risk of inadequate segregation of duties.

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

Answer: D

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

NEW QUESTION 102
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 105
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 107
How is the time required for transaction processing review usually affected by properly implemented Electronic Data Interface (EDI)?

A. EDI usually decreases the time necessary for revie
B. EDI usually increases the time necessary for revie
C. Cannot be determine
D. EDI does not affect the time necessary for revie

Answer: A

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

NEW QUESTION 110
What would an IS auditor expect to find in the console log? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 111
What is essential for the IS auditor to obtain a clear understanding of network management?

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

Answer: C

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

NEW QUESTION 116
How is risk affected if users have direct access to a database at the system level?

A. Risk of unauthorized access increases, but risk of untraceable changes to the database decrease
B. Risk of unauthorized and untraceable changes to the database increase
C. Risk of unauthorized access decreases, but risk of untraceable changes to the database increase
D. Risk of unauthorized and untraceable changes to the database decrease

Answer: B

Explanation: If users have direct access to a database at the system level, risk of unauthorized and untraceable changes to the database increases.

NEW QUESTION 119
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 Interne
B. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a dedicated T1 connectio
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 facilit
D. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a wireless connectio

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 123
What benefit does using capacity-monitoring software to monitor usage patterns and trends provide to management? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 126
What can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 129
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 133
Which of the following best characterizes "worms"?

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

Answer: A

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

NEW QUESTION 135
What is an initial step in creating a proper firewall policy?

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

Answer: C

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

NEW QUESTION 139
What type of cryptosystem is characterized by data being encrypted by the sender using the recipient's public key, and the data then being decrypted using the recipient's private key?

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

Answer: B

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

NEW QUESTION 143
What are used as the framework for developing logical access controls?

A. Information systems security policies
B. Organizational security policies
C. Access Control Lists (ACL)
D. Organizational charts for identifying roles and responsibilities

Answer: A

Explanation: Information systems security policies are used as the framework for developing logical access controls.

NEW QUESTION 144
Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

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

Answer: C

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

NEW QUESTION 148
Which of the following is a good control for protecting confidential data residing on a PC?

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

Answer: C

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

NEW QUESTION 151
Which of the following do digital signatures provide?

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

Answer: A

Explanation: The primary purpose of digital signatures is to provide authentication and integrity of datA.

NEW QUESTION 153
Regarding digital signature implementation, which of the following answers is correct?

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

Answer: C

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

NEW QUESTION 154
What are often the primary safeguards for systems software and data?

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

Answer: B

Explanation: Logical access controls are often the primary safeguards for systems software and datA.
Which of the following is often used as a detection and deterrent control against Internet
attacks? A. Honeypots B. CCTV C. VPN D. VLAN Answer: A Honeypots are often used as a detection and deterrent control against Internet attacks.

NEW QUESTION 155
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 160
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 161
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 163
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 165
What is the key distinction between encryption and hashing algorithms?

A. Hashing algorithms ensure data confidentialit
B. Hashing algorithms are irreversibl
C. Encryption algorithms ensure data integrit
D. Encryption algorithms are not irreversibl

Answer: B

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

NEW QUESTION 169

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

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

Answer: B

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

NEW QUESTION 172
Who is ultimately responsible and accountable for reviewing user access to systems?

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

Answer: C

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

NEW QUESTION 176
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 177
Which of the following is MOST is 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 179
Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

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

Answer: C

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

NEW QUESTION 180
What influences decisions regarding criticality of assets?

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

Answer: C

Explanation: Criticality of assets is often influenced by the business criticality of the data to be protected and by the scope of the impact upon the organization as

a whole. For example, the loss of a network backbone creates a much greater impact on the organization as a whole than the loss of data on a typical user's workstation.

NEW QUESTION 182
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 186
With the objective of mitigating the risk and impact of a major business interruption, a disasterrecovery plan should endeavor to reduce the length of recovery time necessary, as well as costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs. True or false?

A. True
B. False

Answer: A

Explanation: With the objective of mitigating the risk and impact of a major business interruption, a disaster-recovery plan should endeavor to reduce the length of recovery time necessary and the costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs.

NEW QUESTION 191
Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following? Choose the BEST answer.

A. IT strategic plan
B. Business continuity plan
C. Business impact analysis
D. Incident response plan

Answer: B

Explanation: Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of a business continuity plan.

NEW QUESTION 193
What is often the most difficult part of initial efforts in application development? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 194
What is a primary high-level goal for an auditor who is reviewing a system development project?

A. To ensure that programming and processing environments are segregated
B. To ensure that proper approval for the project has been obtained
C. To ensure that business objectives are achieved
D. To ensure that projects are monitored and administrated effectively

Answer: C

Explanation: A primary high-level goal for an auditor who is reviewing a systems-development project is to ensure that business objectives are achieved. This objective guides all other systems development objectives.

NEW QUESTION 197
Whenever an application is modified, what should be tested to determine the full impact of the change? Choose the BEST answer.

A. Interface systems with other applications or systems
B. The entire program, including any interface systems with other applications or systems
C. All programs, including interface systems with other applications or systems
D. Mission-critical functions and any interface systems with other applications or systems

Answer: B

Explanation: Whenever an application is modified, the entire program, including any interface systems with other applications or systems, should be tested to determine the full impact of the change.

NEW QUESTION 201
The quality of the metadata produced from a data warehouse is _____ in the warehouse's design. Choose the BEST answer.

A. Often hard to determine because the data is derived from a heterogeneous data environment
B. The most important consideration
C. Independent of the quality of the warehoused databases
D. Of secondary importance to data warehouse content

Answer: B

Explanation: The quality of the metadata produced from a data warehouse is the most important consideration in the warehouse's design.

NEW QUESTION 205
Who assumes ownership of a systems-development project and the resulting system?

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

Answer: A

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

NEW QUESTION 210
If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

A. Documentation development
B. Comprehensive integration testing
C. Full unit testing
D. Full regression testing

Answer: B

Explanation: If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further comprehensive integration testing.

NEW QUESTION 215
When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 218
What is a reliable technique for estimating the scope and cost of a software-development project?

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

Answer: A

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

NEW QUESTION 223
Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

A. Function Point Analysis (FPA)
B. GANTT
C. Rapid Application Development (RAD)
D. PERT

Answer: D

Explanation: PERT is a program-evaluation review technique that considers different scenarios for planning and control projects.

NEW QUESTION 225
If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 228
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 230
Run-to-run totals can verify data through which stage(s) of application processing?

A. Initial
B. Various
C. Final
D. Output

Answer: B

Explanation: Run-to-run totals can verify data through various stages of application processing.

NEW QUESTION 232
_____ (fill in the blank) is/are are ultimately accountable for the functionality, reliability, and security within IT governance. Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 235
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 239
_____ risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a _____ risk assessment is more appropriate. Fill in the blanks.

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

Answer: A

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

NEW QUESTION 240
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 identifie
C. Relative business processe
D. Relevant application risk

Answer: C

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

NEW QUESTION 241
When storing data archives off-site, what must be done with the data to ensure data completeness?

A. The data must be normalize
B. The data must be validate
C. The data must be parallel-teste
D. The data must be synchronize

Answer: D

Explanation: When storing data archives off-site, data must be synchronized to ensure data completeness.

NEW QUESTION 245
Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

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

Answer: A

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

NEW QUESTION 248
What is an edit check to determine whether a field contains valid data?

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

Answer: A

Explanation: A completeness check is an edit check to determine whether a field contains valid datA.

NEW QUESTION 253
A transaction journal provides the information necessary for detecting unauthorized _____ (fill in the blank) from a terminal.

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

Answer: B

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

NEW QUESTION 256
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 259
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 261
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 264
Parity bits are a control used to validate:

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

Answer: B

Explanation: Parity bits are a control used to validate data completeness.

NEW QUESTION 265
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 270
Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

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

Answer: B

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

NEW QUESTION 274
What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

A. Document existing internal controls
B. Perform compliance testing on internal controls
C. Establish a controls-monitoring steering committee
D. Identify high-risk areas within the organization

Answer: D

Explanation: When implementing continuous-monitoring systems, an IS auditor's first step is to identify highrisk areas within the organization.

NEW QUESTION 278
What type of risk is associated with authorized program exits (trap doors)? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 280
Which of the following is best suited for searching for address field duplications?

A. Text search forensic utility software
B. Generalized audit software
C. Productivity audit software
D. Manual review

Answer: B

Explanation: Generalized audit software can be used to search for address field duplications.

NEW QUESTION 284
Which of the following is of greatest concern to the IS auditor?

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

Answer: A

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

NEW QUESTION 289
An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated datA. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 294
An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

A. True
B. False

Answer: A

Explanation: It is true that an advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions.

NEW QUESTION 295
Why does an IS auditor review an organization chart?

A. To optimize the responsibilities and authority of individuals
B. To control the responsibilities and authority of individuals
C. To better understand the responsibilities and authority of individuals
D. To identify project sponsors

Answer: C

Explanation: The primary reason an IS auditor reviews an organization chart is to better understand the responsibilities and authority of individuals.

NEW QUESTION 298
Ensuring that security and control policies support business and IT objectives is a primary objective of:

A. An IT security policies audit
B. A processing audit
C. A software audit
D. A vulnerability assessment

Answer: A

Explanation: Ensuring that security and control policies support business and IT objectives is a primary objective of an IT security policies audit.

NEW QUESTION 301
When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 305
When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

A. Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic pla
B. Reviewing an audit client's business plan should be performed after reviewing an organization's IT strategic pla
C. Reviewing an audit client's business plan should be performed during the review of an organization's IT strategic pla
D. Reviewing an audit client's business plan should be performed without regard to an organization's IT strategic pla

Answer: A

Explanation: Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.

NEW QUESTION 306
Allowing application programmers to directly patch or change code in production programs increases risk of fraud. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 308
The directory system of a database-management system describes:

A. The access method to the data
B. The location of data AND the access method
C. The location of data
D. Neither the location of data NOR the access method

Answer: B

Explanation: The directory system of a database-management system describes the location of data and the access method.

NEW QUESTION 309
In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

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

Answer: B

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

NEW QUESTION 312
Why is the WAP gateway a component warranting critical concern and review for the IS auditor when auditing and testing controls enforcing message confidentiality?

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

Answer: C

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

NEW QUESTION 317
Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 321
How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

A. Modems convert analog transmissions to digital, and digital transmission to analo
B. Modems encapsulate analog transmissions within digital, and digital transmissions within analo
C. Modems convert digital transmissions to analog, and analog transmissions to digita
D. Modems encapsulate digital transmissions within analog, and analog transmissions within digita

Answer: A

Explanation: Modems (modulation/demodulation) convert analog transmissions to digital, and digital transmissions to analog, and are required for analog transmissions to enter a digital network.

NEW QUESTION 324
Which of the following are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 325
What supports data transmission through split cable facilities or duplicate cable facilities?

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

Answer: A

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

NEW QUESTION 326
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 329
What is an effective control for granting temporary access to vendors and external support personnel? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 332
What is a common vulnerability, allowing denial-of-service attacks?

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

Answer: C

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

NEW QUESTION 334
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 339
Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

A. Traffic analysis
B. SYN flood

C. Denial of service (DoS)
D. Distributed denial of service (DoS)

Answer: A

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

NEW QUESTION 340
Which of the following fire-suppression methods is considered to be the most environmentally friendly?

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

Answer: C

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

NEW QUESTION 345
What is a callback system?

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

Answer: C

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

NEW QUESTION 349
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 350
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 353
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 355
What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

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

Answer: C

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

NEW QUESTION 360
What determines the strength of a secret key within a symmetric key cryptosystem?

A. A combination of key length, degree of permutation, and the complexity of the data-encryption algorithm that uses the key
B. A combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key
C. A combination of key length and the complexity of the data-encryption algorithm that uses the key
D. Initial input vectors and the complexity of the data-encryption algorithm that uses the key

Answer: B

Explanation: The strength of a secret key within a symmetric key cryptosystem is determined by a combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key.

NEW QUESTION 362
What process is used to validate a subject's identity?

A. Identification
B. Nonrepudiation
C. Authorization
D. Authentication

Answer: D

Explanation: Authentication is used to validate a subject's identity.

NEW QUESTION 365
Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 368
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 373
Which of the following is the most fundamental step in preventing virus attacks?

A. Adopting and communicating a comprehensive antivirus policy
B. Implementing antivirus protection software on users' desktop computers
C. Implementing antivirus content checking at all network-to-Internet gateways
D. Inoculating systems with antivirus code

Answer: A

Explanation: Adopting and communicating a comprehensive antivirus policy is the most fundamental step in preventing virus attacks. All other antivirus prevention efforts rely upon decisions established and communicated via policy.

NEW QUESTION 377
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 379
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 380
Rather than simply reviewing the adequacy of access control, appropriateness of access policies, and effectiveness of safeguards and procedures, the IS auditor is more concerned with effectiveness and utilization of assets. True or false?

A. True
B. False

Answer: B

Explanation: Instead of simply reviewing the effectiveness and utilization of assets, an IS auditor is more concerned with adequate access control, appropriate access policies, and effectiveness of safeguards and procedures.

NEW QUESTION 385
If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 389
The purpose of business continuity planning and disaster-recovery planning is to:

A. Transfer the risk and impact of a business interruption or disaster
B. Mitigate, or reduce, the risk and impact of a business interruption or disaster
C. Accept the risk and impact of a business
D. Eliminate the risk and impact of a business interruption or disaster

Answer: B

Explanation: The primary purpose of business continuity planning and disaster-recovery planning is to mitigate, or reduce, the risk and impact of a business interruption or disaster. Total elimination of risk is impossible.

NEW QUESTION 390
If a database is restored from information backed up before the last system image, which of the following is recommended?

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

D. The system should be restarted on the last transactio

Answer: B

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

NEW QUESTION 393
An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

A. True
B. False

Answer: B

Explanation: An off-site processing facility should not be easily identifiable externally because easy identification would create an additional vulnerability for sabotage.

NEW QUESTION 396
How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

A. By implementing redundant systems and applications onsite
B. By geographically dispersing resources
C. By retaining onsite data backup in fireproof vaults
D. By preparing BCP and DRP documents for commonly identified disasters

Answer: B

Explanation: Minimizing single points of failure or vulnerabilities of a common disaster is mitigated by geographically dispersing resources.

NEW QUESTION 401
Mitigating the risk and impact of a disaster or business interruption usually takes priority over transference of risk to a third party such as an insurer. True or false?

A. True
B. False

Answer: A

Explanation: Mitigating the risk and impact of a disaster or business interruption usually takes priority over transferring risk to a third party such as an insurer.

NEW QUESTION 404
What is an acceptable recovery mechanism for extremely time-sensitive transaction processing?

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

Answer: C

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

NEW QUESTION 407
Off-site data backup and storage should be geographically separated so as to _____ (fill in the blank) the risk of a widespread physical disaster such as a hurricane or earthquake.

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

Answer: D

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

NEW QUESTION 412
Why is a clause for requiring source code escrow in an application vendor agreement important?

A. To segregate systems development and live environments

B. To protect the organization from copyright disputes
C. To ensure that sufficient code is available when needed
D. To ensure that the source code remains available even if the application vendor goes out of business

Answer: D

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

NEW QUESTION 417
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 420
Who is ultimately responsible for providing requirement specifications to the software-development team?

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

Answer: A

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

NEW QUESTION 425
What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?

A. Contrived data
B. Independently created data
C. Live data
D. Data from previous tests

Answer: D

Explanation: Regression testing should use data from previous tests to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors.

NEW QUESTION 429
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 434
Which of the following processes are performed during the design phase of the systemsdevelopment life cycle (SDLC) model?

A. Develop test plan
B. Baseline procedures to prevent scope cree
C. Define the need that requires resolution, and map to the major requirements of the solutio
D. Program and test the new syste
E. The tests verify and validate what has been develope

Answer: B

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

NEW QUESTION 436
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 439
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 440
What kind of testing should programmers perform following any changes to an application or system?

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

Answer: A

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

NEW QUESTION 441
What is the most common reason for information systems to fail to meet the needs of users? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 444
Who is responsible for the overall direction, costs, and timetables for systems-development projects?

A. The project sponsor
B. The project steering committee
C. Senior management
D. The project team leader

Answer: B

Explanation: The project steering committee is responsible for the overall direction, costs, and timetables for systems-development projects.

NEW QUESTION 445
When should plans for testing for user acceptance be prepared? Choose the BEST answer.

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

C. In the design phase of the systems-development project
D. In the development phase of the systems-development project

Answer: A

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

NEW QUESTION 450
Authentication techniques for sending and receiving data between EDI systems is crucial to prevent which of the following? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 454
After identifying potential security vulnerabilities, what should be the IS auditor's next step?

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

Answer: C

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

NEW QUESTION 458
What is the primary security concern for EDI environments? Choose the BEST answer.

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

Answer: D

Explanation: Transaction authorization is the primary security concern for EDI environments.

NEW QUESTION 463
Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?

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

Answer: B

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

NEW QUESTION 466
Business process re-engineering often results in _____ automation, which results in _____ number of people using technology. Fill in the blanks.

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

Answer: A

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

NEW QUESTION 469

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

A. True
B. False

Answer: A

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

NEW QUESTION 471
When should an application-level edit check to verify that availability of funds was completed at the electronic funds transfer (EFT) interface?

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

Answer: D

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

NEW QUESTION 474
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 476
What is a data validation edit control that matches input data to an occurrence rate? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 479
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 484
An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

A. variable samplin
B. substantive testin
C. compliance testin
D. stop-or-go samplin

Answer: C

Explanation:
Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were

appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing, such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

NEW QUESTION 486
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 491
Overall business risk for a particular threat can be expressed as:

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

Answer: A

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

NEW QUESTION 494
An audit charter should:

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

Answer: D

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

NEW QUESTION 496
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 testingto confirm whether the quality exists. The other choices are used in substantive testing, which involves testing of details or quantity.

NEW QUESTION 499
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 syste
B. designed an embedded audit module exclusively for auditing the application syste
C. participated as a member of the application system project team, but did not have operational responsibilitie
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 isincorrect because an IS auditor's independence is not impaired by providing advice on known best practices.

NEW QUESTION 500
The PRIMARY advantage of a continuous audit approach is that it:

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

Answer: C

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

NEW QUESTION 505
The PRIMARY purpose of audit trails is to:

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

Answer: B

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

NEW QUESTION 509
When developing a risk-based audit strategy, an IS auditor should conduct a risk assessment to ensure that:

A. controls needed to mitigate risks are in plac
B. vulnerabilities and threats are identifie
C. audit risks are considere
D. a gap analysis is appropriat

Answer: B

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

NEW QUESTION 510
To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

A. schedule the audits and monitor the time spent on each audi
B. train the IS audit staff on current technology used in the compan
C. develop the audit plan on the basis of a detailed risk assessmen
D. monitor progress of audits and initiate cost control measure

Answer: C

Explanation:
Monitoring the time (choice A) and audit programs {choice D), as well as adequate training (choice B), will improve the IS audit staff's productivity (efficiency and performance), but that which delivers value to the organization are the resources and efforts being dedicated to, and focused on, the higher-risk areas.

NEW QUESTION 514
An organization's IS audit charter should specify the:

A. short- and long-term plans for IS audit engagements
B. objectives and scope of IS audit engagement
C. detailed training plan for the IS audit staf
D. role of the IS audit functio

Answer: D

Explanation:
An IS audit charter establishes the role of the information systems audit function. The charter should describe the overall authority, scope, and responsibilities of the audit function. It should be approved by the highest level of management and, if available, by the audit committee. Short-term and long-term planning is the responsibility of audit management. The objectives and scope of each IS audit should be agreed to in an engagement letter. A training plan, based on the audit plan, should be developed by audit management.

NEW QUESTION 515
In planning an audit, the MOST critical step is the identification of the:

A. areas of high ris
B. skill sets of the audit staf
C. test steps in the audi
D. time allotted for the audi

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 auditare 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 518
The extent to which data will be collected during an IS audit should be determined based on the:

A. availability of critical and required informatio
B. auditor's familiarity with the circumstance
C. auditee's ability to find relevant evidenc
D. purpose and scope of the audit being don

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 thescope of the audit should not be limited by the auditee's ability to find relevant evidence.

NEW QUESTION 523
While planning an audit, an assessment of risk should be made to provide:

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

Answer: A

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

NEW QUESTION 526
An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

A. the probability of error must be objectively quantifie
B. the auditor wishes to avoid sampling ris
C. generalized audit software is unavailabl
D. the tolerable error rate cannot be determine

Answer: A

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

audit software. Choice D is incorrect because the tolerable error rate must be predetermined for both judgment and statistical sampling.

NEW QUESTION 531
When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

A. sufficient evidence will be collecte
B. all significant deficiencies identified will be corrected within a reasonable perio
C. all material weaknesses will be identifie
D. audit costs will be kept at a minimum leve

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 533
An IS auditor evaluating logical access controls should FIRST:

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

Answer: D

Explanation:
When evaluating logical access controls, an IS auditor should first obtain an understanding of the security risks facing information processing by reviewing relevant documentation, by inquiries, and by conducting a risk assessment. Documentation andevaluation is the second step in assessing the adequacy, efficiency and effectiveness, thus identifying deficiencies or redundancy in controls. The third step is to test the access paths-to determine if the controls are functioning. Lastly, theIS auditor evaluates the security environment to assess its adequacy by reviewing the written policies, observing practices and comparing them to appropriate security best practices.

NEW QUESTION 538
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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