



Isaca

Exam Questions CISA

Isaca CISA

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 2

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 3

- (Topic 1)

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 4

- (Topic 1)

A hub is a device that connects:

- A. two LANs using different protocol
- B. a LAN with a WA
- C. a LAN with a metropolitan area network (MAN).
- D. two segments of a single LA

Answer: D

Explanation:

A hub is a device that connects two segments of a single LAN. A hub is a repeater. It provides transparent connectivity to users on all segments of the same LAN. It is a level 1 device.

NEW QUESTION 5

- (Topic 1)

A LAN administrator normally would be restricted from:

- A. having end-user responsibilitie
- B. reporting to the end-user manage
- C. having programming responsibilitie
- D. being responsible for LAN security administratio

Answer: C

Explanation:

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

NEW QUESTION 6

- (Topic 1)

A malicious code that changes itself with each file it infects is called a:

- A. logic bom
- B. stealth viru
- C. trojan hors
- D. polymorphic viru

Answer: D

Explanation:

A polymorphic virus has the capability of changing its own code, enabling it to have many different variants. Since they have no consistent binary pattern, such viruses are hard to identify.

NEW QUESTION 7

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 8

- (Topic 1)

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 9

- (Topic 1)

IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

- A. True
- B. False

Answer: A

Explanation:

IS auditors are most likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. Think of it this way: If any reliance is placed on internal controls, that reliance must be validated through compliance testing. High control risk results in little reliance on internal controls, which results in additional substantive testing.

NEW QUESTION 10

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 10

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 11

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 12

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 16

- (Topic 1)

Why does the IS auditor often review the system logs?

- A. To get evidence of password spoofing
- B. To get evidence of data copy activities
- C. To determine the existence of unauthorized access to data by a user or program
- D. To get evidence of password sharing

Answer: C

Explanation:

When trying to determine the existence of unauthorized access to data by a user or program, the IS auditor will often review the system logs.

NEW QUESTION 19

- (Topic 1)

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 23

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 25

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 27

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 30

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 33

- (Topic 1)

What is the key distinction between encryption and hashing algorithms?

- A. Hashing algorithms ensure data confidentiality
- B. Hashing algorithms are irreversible
- C. Encryption algorithms ensure data integrity
- D. Encryption algorithms are not irreversible

Answer: B

Explanation:

A key distinction between encryption and hashing algorithms is that hashing

algorithms are irreversible.

NEW QUESTION 34

- (Topic 1)

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 37

- (Topic 1)

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 38

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 41

- (Topic 1)

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

- A. True
- B. False

Answer: B

Explanation:

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

NEW QUESTION 45

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 47

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 49

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 53

- (Topic 1)

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 56

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 61

- (Topic 1)

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 62

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 64

- (Topic 1)

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

Answer: A

Explanation:

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

NEW QUESTION 68

- (Topic 1)

The directory system of a database-management system describes:

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

Answer: B

Explanation:

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

NEW QUESTION 71

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 74

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 76

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 77

- (Topic 1)

What can be used to gather evidence of network attacks?

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

Answer: B

Explanation:

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

NEW QUESTION 81

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 82

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 86

- (Topic 1)

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

- A. False
- B. True

Answer: B

Explanation:

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

NEW QUESTION 91

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 96

- (Topic 1)

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 99

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 104

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 108

- (Topic 1)

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 110

- (Topic 1)

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 113

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 115

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 120

- (Topic 1)

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 122

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 126

- (Topic 1)

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 130

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 131

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 135

- (Topic 1)

_____ (fill in the blank) should be implemented as early as data preparation to support data integrity at the earliest point possible.

- A. Control totals
- B. Authentication controls
- C. Parity bits
- D. Authorization controls

Answer: A

Explanation:

Control totals should be implemented as early as data preparation to support data integrity at the earliest point possible.

NEW QUESTION 138

- (Topic 1)

Data edits are implemented before processing and are considered which of the following? Choose the BEST answer.

- A. Deterrent integrity controls
- B. Detective integrity controls
- C. Corrective integrity controls
- D. Preventative integrity controls

Answer: D

Explanation:

Data edits are implemented before processing and are considered preventive integrity controls.

NEW QUESTION 141

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 142

- (Topic 2)

Which of the following is a substantive test?

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

Answer: C

Explanation:

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

NEW QUESTION 145

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 148

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 150

- (Topic 2)

During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

- A. create the procedures document
- B. terminate the audit
- C. conduct compliance testing
- D. identify and evaluate existing practices

Answer: D

Explanation:

One of the main objectives of an audit is to identify potential risks; therefore, the most proactive approach would be to identify and evaluate the existing security practices being followed by the organization. IS auditors should not prepare documentation, as doing so could jeopardize their independence. Terminating the audit may prevent achieving one of the basic audit objectives, i.e., identification of potential risks. Since there are no documented procedures, there is no basis against which to test compliance.

NEW QUESTION 155

- (Topic 2)

An integrated test facility is considered a useful audit tool because it:

- A. is a cost-efficient approach to auditing application control
- B. enables the financial and IS auditors to integrate their audit tests
- C. compares processing output with independently calculated data
- D. provides the IS auditor with a tool to analyze a large range of information

Answer: C

Explanation:

An integrated test facility is considered a useful audit tool because it uses the same programs to compare processing using independently calculated data. This involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.

NEW QUESTION 160

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 165

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 169

- (Topic 2)

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

- A. understand the business proces
- B. comply with auditing standard
- C. identify control weaknes
- D. plan substantive testin

Answer: A

Explanation:

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

NEW QUESTION 173

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 178

- (Topic 2)

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

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

Answer: B

Explanation:

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

investigation. An analytical review assesses the general control environment of an organization.

NEW QUESTION 183

- (Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 186

- (Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 189

- (Topic 2)

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

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

Answer: D

Explanation:

ISACA's standard on 'reporting' requires the IS auditor have sufficient and appropriate audit evidence to support the reported results. Statements from IS management provide a basis for obtaining concurrence on matters that cannot be verified with empirical evidence. The report should be based on evidence collected during the course of the review even though the auditor may have access to the work papers of other auditors. The results of an organizational control self-assessment (CSA) could supplement the audit findings. Choices A, B and C might be referenced during an audit but, of themselves, would not be considered a sufficient basis for issuing a report.

NEW QUESTION 190

- (Topic 2)

Which of the following is an attribute of the control self-assessment (CSA) approach?

- A. Broad stakeholder involvement
- B. Auditors are the primary control analysts
- C. Limited employee participation
- D. Policy driven

Answer: A

Explanation:

The control self-assessment (CSA) approach emphasizes management of and accountability for developing and monitoring the controls of an organization's business processes. The attributes of CSA include empowered employees, continuous improvement, extensive employee participation and training, all of which are representations of broad stakeholder involvement. Choices B, C and D are attributes of a traditional audit approach.

NEW QUESTION 193

- (Topic 3)

An IS steering committee should:

- A. include a mix of members from different departments and staff level
- B. ensure that IS security policies and procedures have been executed properly
- C. have formal terms of reference and maintain minutes of its meeting
- D. be briefed about new trends and products at each meeting by a vendor

Answer: C

Explanation:

It is important to keep detailed steering committee minutes to document the decisions and activities of the IS steering committee, and the board of directors should be informed about those decisions on a timely basis. Choice A is incorrect because only senior management or high-level staff members should be on this committee because of its strategic mission. Choice B is not a responsibility of this committee, but the responsibility of the security administrator. Choice D is incorrect because a vendor should be invited to meetings only when appropriate.

NEW QUESTION 198

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 200

- (Topic 3)

When implementing an IT governance framework in an organization the MOST important objective is:

- A. IT alignment with the business
- B. accountability
- C. value realization with IT
- D. enhancing the return on IT investment

Answer: A

Explanation:

The goals of IT governance are to improve IT performance, to deliver optimum business value and to ensure regulatory compliance. The key practice in support of these goals is the strategic alignment of IT with the business (choice A). To achieve alignment, all other choices need to be tied to business practices and strategies.

NEW QUESTION 204

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 209

- (Topic 3)

Responsibility for the governance of IT should rest with the:

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

Answer: D

Explanation:

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

organization, but the ultimate accountability resides with the board of directors.

NEW QUESTION 214

- (Topic 3)

An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

- A. User acceptance testing (UAT) occur for all reports before release into production
- B. Organizational data governance practices be put in place
- C. Standard software tools be used for report development
- D. Management sign-off on requirements for new reports

Answer: B

Explanation:

This choice directly addresses the problem. An organizationwide approach is needed to achieve effective management of data assets. This includes enforcing standard definitions of data elements, which is part of a data governance initiative. The other choices, while sound development practices, do not address the root cause of the problem described.

NEW QUESTION 218

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 222

- (Topic 3)

Which of the following would BEST provide assurance of the integrity of new staff?

- A. Background screening
- B. References
- C. Bonding
- D. Qualifications listed on a resume

Answer: A

Explanation:

A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a resume may not be accurate.

NEW QUESTION 226

- (Topic 3)

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

- A. ensure the employee maintains a good quality of life, which will lead to greater productivity
- B. reduce the opportunity for an employee to commit an improper or illegal act
- C. provide proper cross-training for another employee
- D. eliminate the potential disruption caused when an employee takes vacation one day at a time

Answer: B

Explanation:

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

NEW QUESTION 229

- (Topic 3)

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

- A. having end-user responsibilitie
- B. reporting to the end-user manage
- C. having programming responsibilitie
- D. being responsible for LAN security administratio

Answer: C

Explanation:

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

NEW QUESTION 230

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 234

- (Topic 3)

Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?

- A. Allocating resources
- B. Keeping current with technology advances
- C. Conducting control self-assessment
- D. Evaluating hardware needs

Answer: A

Explanation:

The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department.

NEW QUESTION 238

- (Topic 3)

To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

- A. the IT infrastrucur
- B. organizational policies, standards and procedure
- C. legal and regulatory requirement
- D. the adherence to organizational policies, standards and procedure

Answer: C

Explanation:

To ensure that the organization is complying with privacy issues, an IS auditor should address legal and regulatory requirements first. To comply with legal and regulatory requirements, organizations need to adopt the appropriate infrastructure. After understanding the legal and regulatory requirements, an IS auditor should evaluate organizational policies, standards and procedures to determine whether they adequately address the privacy requirements, and then review the adherence to these specific policies, standards and procedures.

NEW QUESTION 239

- (Topic 3)

To assist an organization in planning for IT investments, an IS auditor should recommend the use of:

- A. project management tool
- B. an object-oriented architectur
- C. tactical plannin
- D. enterprise architecture (EA).

Answer: D

Explanation:

Enterprise architecture (EA) involves documenting the organization's IT assets and processes in a structured manner to facilitate understanding, management and planning for IT investments. It involves both a current state and a representation of an optimized future state. In attempting to complete an EA, organizations can address the problem either from a technology perspective or a business process perspective. Project management does not consider IT investment aspects; it is a tool to aid in delivering projects. Object-oriented architecture is a software development methodology and does not assist in planning for IT investment, while tactical planning is relevant only after high-level IT investment decisions have been made.

NEW QUESTION 241

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 242

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 244

- (Topic 3)

To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

- A. O/S and hardware refresh frequencies
- B. Gain-sharing performance bonuses
- C. Penalties for noncompliance
- D. Charges tied to variable cost metrics

Answer: B

Explanation:

Because the outsourcer will share a percentage of the achieved savings, gain-sharing performance bonuses provide a financial incentive to go above and beyond the stated terms of the contract and can lead to cost savings for the client. Refresh frequencies and penalties for noncompliance would only encourage the outsourcer to meet minimum requirements. Similarly, tying charges to variable cost metrics would not encourage the outsourcer to seek additional efficiencies that might benefit the client.

NEW QUESTION 249

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 250

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 251

- (Topic 3)

When developing a risk management program, what is the FIRST activity to be performed?

- A. Threat assessment
- B. Classification of data
- C. Inventory of assets
- D. Criticality analysis

Answer: C

Explanation:

Identification of the assets to be protected is the first step in the development of a risk management program. A listing of the threats that can affect the performance of these assets and criticality analysis are later steps in the process. Data classification is required for defining access controls and in criticality analysis.

NEW QUESTION 253

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 257

- (Topic 4)

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

- A. a clear business case has been approved by managemen
- B. corporate security standards will be me
- C. users will be involved in the implementation pla
- D. the new system will meet all required user functionalit

Answer: A

Explanation:

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

NEW QUESTION 259

- (Topic 4)

Which of the following risks could result from inadequate software baselining?

- A. Scope creep
- B. Sign-off delays
- C. Software integrity violations
- D. inadequate controls

Answer: A

Explanation:

A software baseline is the cut-off point in the design and development of a system beyond which additional requirements or modifications to the design do not or cannot occur without undergoing formal strict procedures for approval based on a business cost-benefit analysis. Failure to adequately manage the requirements of a system through baselining can result in a number of risks. Foremost among these risks is scope creep, the process through which requirements change during development. Choices B, C and D may not always result, but choice A is inevitable.

NEW QUESTION 261

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 262

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 264

- (Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 266

- (Topic 4)

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

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

Answer: B

Explanation:

Earned value analysis (EVA) is an industry standard method for measuring a project's progress at any given point in time, forecasting its completion date and final cost, and analyzing variances in the schedule and budget as the project proceeds. It compares the planned amount of work with what has actually been completed, to determine if the cost, schedule and work accomplished are progressing in accordance with the plan. EVA works most effectively if a well-formed

work breakdown structure exists. Function point analysis (FPA) is an indirect measure of software size and complexity and, therefore, does not address the elements of time and budget. Cost budgets do not address time. PERT aids in time and deliverables management, but lacks projections for estimates at completion (EACs) and overall financial management.

NEW QUESTION 269

- (Topic 4)

When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

- A. project be discontinued
- B. business case be updated and possible corrective actions be identified
- C. project be returned to the project sponsor for reapproval
- D. project be completed and the business case be updated later

Answer: B

Explanation:

An IS auditor should not recommend discontinuing or completing the project before reviewing an updated business case. The IS auditor should recommend that the business case be kept current throughout the project since it is a key input to decisions made throughout the life of any project.

NEW QUESTION 272

- (Topic 4)

Which of the following situations would increase the likelihood of fraud?

- A. Application programmers are implementing changes to production program
- B. Application programmers are implementing changes to test program
- C. Operations support staff are implementing changes to batch schedule
- D. Database administrators are implementing changes to data structure

Answer: A

Explanation:

Production programs are used for processing an enterprise's data. It is imperative that controls on changes to production programs are stringent. Lack of control in this area could result in application programs being modified to manipulate the data. Application programmers are required to implement changes to test programs. These are used only in development and do not directly impact the live processing of data. The implementation of changes to batch schedules by operations support staff will affect the scheduling of the batches only; it does not impact the live data. Database administrators are required to implement changes to data structures. This is required for reorganization of the database to allow for additions, modifications or deletions of fields or tables in the database.

NEW QUESTION 274

- (Topic 4)

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

- A. integrity
- B. authenticity
- C. authorization
- D. nonrepudiation

Answer: A

Explanation:

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

NEW QUESTION 278

- (Topic 4)

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

- A. satisfy a requirement in addressing a risk issue
- B. do not reduce productivity
- C. are based on a cost-benefit analysis
- D. are detective or corrective

Answer: A

Explanation:

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

NEW QUESTION 279

- (Topic 4)

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

- A. Uncontrolled multiple software versions

- B. Source programs that are not synchronized with object code
- C. incorrectly set parameters
- D. Programming error

Answer: C

Explanation:

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

NEW QUESTION 280

- (Topic 4)

A decision support system (DSS):

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

Answer: C

Explanation:

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

NEW QUESTION 281

- (Topic 4)

An IS auditor's PRIMARY concern when application developers wish to use a copy of yesterday's production transaction file for volume tests is that:

- A. users may prefer to use contrived data for testin
- B. unauthorized access to sensitive data may resul
- C. error handling and credibility checks may not be fully prove
- D. the full functionality of the new process may not necessarily be teste

Answer: B

Explanation:

Unless the data are sanitized, there is a risk of disclosing sensitive data.

NEW QUESTION 282

- (Topic 4)

Which of the following is the PRIMARY purpose for conducting parallel testing?

- A. To determine if the system is cost-effective
- B. To enable comprehensive unit and system testing
- C. To highlight errors in the program interfaces with files
- D. To ensure the new system meets user requirements

Answer: D

Explanation:

The purpose of parallel testing is to ensure that the implementation of a new system will meet user requirements. Parallel testing may show that the old system is, in fact, better than the new system, but this is not the primary reason. Unit and system testing are completed before parallel testing. Program interfaces with files are tested for errors during system testing.

NEW QUESTION 284

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 287

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 290

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 292

- (Topic 4)

A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

- A. Key verification
- B. One-for-one checking
- C. Manual recalculations
- D. Functional acknowledgements

Answer: D

Explanation:

Acting as an audit trail for EDI transactions, functional acknowledgements are one of the main controls used in data mapping. All the other choices are manual input controls, whereas data mapping deals with automatic integration of data in the receiving company.

NEW QUESTION 293

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 297

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 302

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 307

- (Topic 4)

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

- A. review the integrity of system access control
- B. accept management's statement that effective access controls are in place
- C. stress the importance of having a system control framework in place
- D. review the background checks of the accounts payable staff

Answer: C

Explanation:

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

NEW QUESTION 310

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 312

- (Topic 5)

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

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

D. Number of agents answering the phones

Answer: B

Explanation:

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

NEW QUESTION 314

- (Topic 5)

During a human resources (HR) audit, an IS auditor is informed that there is a verbal agreement between the IT and HR departments as to the level of IT services expected. In this situation, what should the IS auditor do FIRST?

- A. Postpone the audit until the agreement is documented
- B. Report the existence of the undocumented agreement to senior management
- C. Confirm the content of the agreement with both departments
- D. Draft a service level agreement (SLA) for the two departments

Answer: C

Explanation:

An IS auditor should first confirm and understand the current practice before making any recommendations. The agreement can be documented after it has been established that there is an agreement in place. The fact that there is not a written agreement does not justify postponing the audit, and reporting to senior management is not necessary at this stage of the audit. Drafting a service level agreement (SLA) is not the IS auditor's responsibility.

NEW QUESTION 319

- (Topic 5)

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

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

Answer: A

Explanation:

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

NEW QUESTION 321

- (Topic 5)

The MOST significant security concern when using flash memory (e.g., USB removable disk) is that the:

- A. contents are highly volatile
- B. data cannot be backed up
- C. data can be copied
- D. device may not be compatible with other peripheral

Answer: C

Explanation:

Unless properly controlled, flash memory provides an avenue for anyone to copy any content with ease. The contents stored in flash memory are not volatile. Backing up flash memory data is not a control concern, as the data are sometimes stored as a backup. Flash memory will be accessed through a PC rather than any other peripheral; therefore, compatibility is not an issue.

NEW QUESTION 325

- (Topic 5)

A database administrator has detected a performance problem with some tables which could be solved through denormalization. This situation will increase the risk of:

- A. concurrent access
- B. deadlock
- C. unauthorized access to data
- D. a loss of data integrity

Answer: D

Explanation:

Normalization is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create redundancy and a risk of not maintaining consistency of data, with the consequent loss of data integrity. Deadlocks are not caused by denormalization. Access to data is controlled by defining user rights to information, and is not affected by denormalization.

NEW QUESTION 326

- (Topic 5)

An IS auditor finds that client requests were processed multiple times when received from different independent departmental databases, which are synchronized weekly. What would be the BEST recommendation?

- A. increase the frequency for data replication between the different department systems to ensure timely update
- B. Centralize all request processing in one department to avoid parallel processing of the same request
- C. Change the application architecture so that common data are held in just one shared database for all department
- D. implement reconciliation controls to detect duplicates before orders are processed in the system

Answer: C

Explanation:

Keeping the data in one place is the best way to ensure that data are stored without redundancy and that all users have the same data on their systems. Although increasing the frequency may help to minimize the problem, the risk of duplication cannot be eliminated completely because parallel data entry is still possible. Business requirements will most likely dictate where data processing activities are performed. Changing the business structure to solve an IT problem is not practical or politically feasible. Detective controls do not solve the problem of duplicate processing, and would require that an additional process be implemented to handle the discovered duplicates.

NEW QUESTION 327

- (Topic 5)

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

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

Answer: D

Explanation:

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

NEW QUESTION 330

- (Topic 5)

Which of the following is MOST directly affected by network performance monitoring tools?

- A. Integrity
- B. Availability
- C. Completeness
- D. Confidentiality

Answer: B

Explanation:

In case of a disruption in service, one of the key functions of network performance monitoring tools is to ensure that the information has remained unaltered. It is a function of security monitoring to assure confidentiality by using such tools as encryption. However, the most important aspect of network performance is assuring the ongoing dependence on connectivity to run the business. Therefore, the characteristic that benefits the most from network monitoring is availability.

NEW QUESTION 333

- (Topic 5)

Change management procedures are established by IS management to:

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

Answer: A

Explanation:

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

NEW QUESTION 334

- (Topic 5)

An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered

an adequate set of compensating controls?

- A. Allow changes to be made only with the DBA user account
- B. Make changes to the database after granting access to a normal user account
- C. Use the DBA user account to make changes, log the changes and review the change log the following day
- D. Use the normal user account to make changes, log the changes and review the change log the following day

Answer: C

Explanation:

The use of a database administrator (DBA) user account is normally set up to log all changes made and is most appropriate for changes made outside of normal hours. The use of a log, which records the changes, allows changes to be reviewed. The use of the DBA user account without logging would permit uncontrolled changes to be made to databases once access to the account was obtained. The use of a normal user account with no restrictions would allow uncontrolled changes to any of the databases. Logging would only provide information on changes made, but would not limit changes to only those that were authorized. Hence, logging coupled with review form an appropriate set of compensating controls.

NEW QUESTION 338

- (Topic 5)

The purpose of code signing is to provide assurance that:

- A. the software has not been subsequently modified
- B. the application can safely interface with another signed application
- C. the signer of the application is trusted
- D. the private key of the signer has not been compromised

Answer: A

Explanation:

Code signing can only ensure that the executable code has not been modified after being signed. The other choices are incorrect and actually represent potential and exploitable weaknesses of code signing.

NEW QUESTION 342

- (Topic 5)

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

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

Answer: A

Explanation:

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

NEW QUESTION 346

- (Topic 5)

Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits vulnerability in a protocol?

- A. Install the vendor's security fix for the vulnerability
- B. Block the protocol traffic in the perimeter firewall
- C. Block the protocol traffic between internal network segment
- D. Stop the service until an appropriate security fix is installed

Answer: D

Explanation:

Stopping the service and installing the security fix is the safest way to prevent the worm from spreading, if the service is not stopped, installing the fix is not the most effective method because the worm continues spreading until the fix becomes effective. Blocking the protocol on the perimeter does not stop the worm from spreading to the internal network(s). Blocking the protocol helps to slow down the spreading but also prohibits any software that utilizes it from working between segments.

NEW QUESTION 351

- (Topic 5)

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

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

D. VLANs

Answer: A

Explanation:

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

NEW QUESTION 353

- (Topic 5)

In a client-server architecture, a domain name service (DNS) is MOST important because it provides the:

- A. address of the domain serve
- B. resolution service for the name/addresses
- C. IP addresses for the internet
- D. domain name system

Answer: B

Explanation:

DNS is utilized primarily on the Internet for resolution of the name/address of the web site. It is an Internet service that translates domain names into IP addresses. As names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time a domain name is used, a DNS service must translate the name into the corresponding IP address. The DNS system has its own network, if one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

NEW QUESTION 354

- (Topic 5)

The most likely error to occur when implementing a firewall is:

- A. incorrectly configuring the access list
- B. compromising the passwords due to social engineering
- C. connecting a modem to the computers in the network
- D. inadequately protecting the network and server from virus attack

Answer: A

Explanation:

An updated and flawless access list is a significant challenge and, therefore, has the greatest chance for errors at the time of the initial installation. Passwords do not apply to firewalls, a modem bypasses a firewall and a virus attack is not an element in implementing a firewall.

NEW QUESTION 357

- (Topic 5)

Which of the following types of transmission media provide the BEST security against unauthorized access?

- A. Copper wire
- B. Twisted pair
- C. Fiberoptic cables
- D. Coaxial cables

Answer: C

Explanation:

Fiberoptic cables have proven to be more secure than the other media. A. Satellite transmission and copper wire can be violated with inexpensive equipment. Coaxial cable can also be violated more easily than other transmission media.

NEW QUESTION 360

- (Topic 5)

Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

- A. Review the parameter setting
- B. Interview the firewall administrator
- C. Review the actual procedure
- D. Review the device's log file for recent attack

Answer: A

Explanation:

A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide audit evidence documentation. The other choices do not provide audit evidence as strong as choice A.

NEW QUESTION 365

- (Topic 5)

An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?

- A. Simple Object Access Protocol (SOAP)
- B. Address Resolution Protocol (ARP)
- C. Routing Information Protocol (RIP)
- D. Transmission Control Protocol (TCP)

Answer: B

Explanation:

Address Resolution Protocol (ARP) provides dynamic address mapping between an IP address and hardware address. Simple Object Access Protocol (SOAP) is a platform-independent XML-based protocol, enabling applications to communicate with each other over the Internet, and does not deal with media access control (MAC) addresses. Routing Information Protocol (RIP) specifies how routers exchange routing table information. Transmission Control Protocol (TCP) enables two hosts to establish a connection and exchange streams of data.

NEW QUESTION 366

- (Topic 5)

During the audit of a database server, which of the following would be considered the GREATEST exposure?

- A. The password does not expire on the administrator account
- B. Default global security settings for the database remain unchanged
- C. Old data have not been purged
- D. Database activity is not fully logged

Answer: B

Explanation:

Default security settings for the database could allow issues like blank user passwords or passwords that were the same as the username. Logging all database activity is not practical. Failure to purge old data may present a performance issue but is not an immediate security concern. Choice A is an exposure but not as serious as B.

NEW QUESTION 367

- (Topic 6)

The GREATEST risk when end users have access to a database at its system level, instead of through the application, is that the users can:

- A. make unauthorized changes to the database directly, without an audit trail
- B. make use of a system query language (SQL) to access information
- C. remotely access the database
- D. update data without authentication

Answer: A

Explanation:

Having access to the database could provide access to database utilities, which can update the database without an audit trail and without using the application. Using SQL only provides read access to information, in a networked environment, accessing the database remotely does not make a difference. What is critical is what is possible or completed through this access. To access a database, it is necessary that a user is authenticated using a user ID.

NEW QUESTION 370

- (Topic 6)

What is the MOST effective method of preventing unauthorized use of data files?

- A. Automated file entry
- B. Tape librarian
- C. Access control software
- D. Locked library

Answer: C

Explanation:

Access control software is an active control designed to prevent unauthorized access to data.

NEW QUESTION 372

- (Topic 6)

Which of the following is the PRIMARY safeguard for securing software and data within an information processing facility?

- A. Security awareness
- B. Reading the security policy
- C. Security committee

D. Logical access controls

Answer: D

Explanation:

To retain a competitive advantage and meet basic business requirements, organizations must ensure that the integrity of the information stored on their computer systems preserve the confidentiality of sensitive data and ensure the continued availability of their information systems. To meet these goals, logical access controls must be in place. Awareness (choice A) itself does not protect against unauthorized access or disclosure of information. Knowledge of an information systems security policy (choice B), which should be known by the organization's employees, would help to protect information, but would not prevent the unauthorized access of information. A security committee (choice C) is key to the protection of information assets, but would address security issues within a broader perspective.

NEW QUESTION 373

- (Topic 6)

Which of the following is a benefit of using a callback device?

- A. Provides an audit trail
- B. Can be used in a switchboard environment
- C. Permits unlimited user mobility
- D. Allows 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 378

- (Topic 6)

The PRIMARY objective of a logical access control review is to:

- A. review access controls provided through software
- B. ensure access is granted per the organization's authorities
- C. walk through and assess the access provided in the IT environment
- D. provide assurance that computer hardware is adequately protected against abuse

Answer: B

Explanation:

The scope of a logical access control review is primarily to determine whether or not access is granted per the organization's authorizations. Choices A and C relate to procedures of a logical access control review, rather than objectives. Choice D is relevant to a physical access control review.

NEW QUESTION 382

- (Topic 6)

Electromagnetic emissions from a terminal represent an exposure because they:

- A. affect noise pollution
- B. disrupt processor function
- C. produce dangerous levels of electric current
- D. can be detected and displayed

Answer: D

Explanation:

Emissions can be detected by sophisticated equipment and displayed, thus giving unauthorized persons access to data. They should not cause disruption of CPUs or effect noise pollution.

NEW QUESTION 384

- (Topic 6)

Security administration procedures require read-only access to:

- A. access control table
- B. security log file
- C. logging option
- D. user profile

Answer: B

Explanation:

Security administration procedures require read-only access to security log files to ensure that, once generated, the logs are not modified. Logs provide evidence and track suspicious transactions and activities. Security administration procedures require write access to access control tables to manage and update the privileges according to authorized business requirements. Logging options require write access to allow the administrator to update the way the transactions and

user activities are monitored, captured, stored, processed and reported.

NEW QUESTION 385

- (Topic 6)

A hacker could obtain passwords without the use of computer tools or programs through the technique of:

- A. social engineering
- B. sniffer
- C. back door
- D. Trojan horse

Answer: A

Explanation:

Social engineering is based on the divulgence of private information through dialogues, interviews, inquiries, etc., in which a user may be indiscreet regarding their or someone else's personal data. A sniffer is a computer tool to monitor the traffic in networks. Back doors are computer programs left by hackers to exploit vulnerabilities. Trojan horses are computer programs that pretend to supplant a real program; thus, the functionality of the program is not authorized and is usually malicious in nature.

NEW QUESTION 390

- (Topic 6)

The implementation of access controls FIRST requires:

- A. a classification of IS resource
- B. the labeling of IS resource
- C. the creation of an access control list
- D. an inventory of IS resource

Answer: D

NEW QUESTION 395

- (Topic 6)

Which of the following is an example of the defense in-depth security principle?

- A. Using two firewalls of different vendors to consecutively check the incoming network traffic
- B. Using a firewall as well as logical access controls on the hosts to control incoming network traffic
- C. Having no physical signs on the outside of a computer center building
- D. Using two firewalls in parallel to check different types of incoming traffic

Answer: B

Explanation:

Defense in-depth means using different security mechanisms that back each other up. When network traffic passes the firewall unintentionally, the logical access controls form a second line of defense. Using two firewalls of different vendors to consecutively check the incoming network traffic is an example of diversity in defense. The firewalls are the same security mechanisms. By using two different products the probability of both products having the same vulnerabilities is diminished. Having no physical signs on the outside of a computer center building is a single security measure. Using two firewalls in parallel to check different types of incoming traffic is a single security mechanism and therefore no different than having a single firewall checking all traffic.

NEW QUESTION 397

- (Topic 6)

An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:

- A. more than one individual can claim to be a specific user
- B. there is no way to limit the functions assigned to user
- C. user accounts can be shared
- D. users have a need-to-know privilege

Answer: B

Explanation:

Without an appropriate authorization process, it will be impossible to establish functional limits and accountability. The risk that more than one individual can claim to be a specific user is associated with the authentication processes, rather than with authorization. The risk that user accounts can be shared is associated with identification processes, rather than with authorization. The need-to-know basis is the best approach to assigning privileges during the authorization process.

NEW QUESTION 402

- (Topic 6)

Which of the following is the BEST method for preventing the leakage of confidential information in a laptop computer?

- A. Encrypt the hard disk with the owner's public key
- B. Enable the boot password (hardware-based password).
- C. Use a biometric authentication device
- D. Use two-factor authentication to logon to the notebook

Answer: A

Explanation:

Only encryption of the data with a secure key will prevent the loss of confidential information. In such a case, confidential information can be accessed only with knowledge of the owner's private key, which should never be shared. Choices B, C and D deal with authentication and not with confidentiality of information. An individual can remove the hard drive from the secured laptop and install it on an unsecured computer, gaining access to the data.

NEW QUESTION 406

- (Topic 6)

An IS auditor finds that a DBA has read and write access to production data. The IS auditor should:

- A. accept the DBA access as a common practice
- B. assess the controls relevant to the DBA function
- C. recommend the immediate revocation of the DBA access to production data
- D. review user access authorizations approved by the DB

Answer: B

Explanation:

It is good practice when finding a potential exposure to look for the best controls. Though granting the database administrator (DBA) access to production data might be a common practice, the IS auditor should evaluate the relevant controls. The DBA should have access based on a need-to-know and need-to-do basis; therefore, revocation may remove the access required. The DBA, typically, may need to have access to some production data. Granting user authorizations is the responsibility of the data owner and not the DBA.

NEW QUESTION 409

- (Topic 6)

An IS auditor has completed a network audit. Which of the following is the MOST significant logical security finding?

- A. Network workstations are not disabled automatically after a period of inactivity
- B. Wiring closets are left unlocked
- C. Network operating manuals and documentation are not properly secure
- D. Network components are not equipped with an uninterruptible power supply

Answer: A

Explanation:

Choice A is the only logical security finding. Network logical security controls should be in place to restrict, identify, and report authorized and unauthorized users of the network. Disabling inactive workstations restricts users of the network. Choice D is an environmental issue and choices B and C are physical security issues. Choices B, C and D should be reported to the appropriate entity.

NEW QUESTION 410

- (Topic 6)

Which of the following would be the BEST overall control for an Internet business looking for confidentiality, reliability and integrity of data?

- A. Secure Sockets Layer (SSL)
- B. Intrusion detection system (IDS)
- C. Public key infrastructure (PKI)
- D. Virtual private network (VPN)

Answer: C

Explanation:

PKI would be the best overall technology because cryptography provides for encryption, digital signatures and non repudiation controls for confidentiality and reliability. SSL can provide confidentiality. IDS is a detective control. A VPN would provide confidentiality and authentication (reliability).

NEW QUESTION 412

- (Topic 6)

To ensure message integrity, confidentiality and non repudiation between two parties, the MOST effective method would be to create a message digest by applying a cryptographic hashing algorithm against:

- A. the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key by using the receiver's public key
- B. any part of the message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key using the receiver's public key
- C. the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering both the encrypted message and digest using the receiver's public key
- D. the entire message, enciphering the message digest using the sender's private key and enciphering the message using the receiver's public key

Answer: A

Explanation:

Applying a cryptographic hashing algorithm against the entire message addresses the message integrity issue. Enciphering the message digest using the sender's private key addresses non repudiation. Encrypting the message with a symmetric key, thereafter allowing the key to be enciphered using the receiver's public key, most efficiently addresses the confidentiality of the message as well as the receiver's non repudiation. The other choices would address only a portion of the requirements.

NEW QUESTION 417

- (Topic 6)

Which of the following would be of MOST concern to an IS auditor reviewing a virtual private network (VPN) implementation? Computers on the network that are located:

- A. on the enterprise's internal network
- B. at the backup site
- C. in employees' home
- D. at the enterprise's remote office

Answer: C

Explanation:

One risk of a virtual private network (VPN) implementation is the chance of allowing high-risk computers onto the enterprise's network. All machines that are allowed onto the virtual network should be subject to the same security policy. Home computers are least subject to the corporate security policies, and therefore are high-risk computers. Once a computer is hacked and 'owned' any network that trusts that computer is at risk. Implementation and adherence to corporate security policy is easier when all computers on the network are on the enterprise's campus. On an enterprise's internal network, there should be security policies in place to detect and halt an outside attack that uses an internal machine as a staging platform. Computers at the backup site are subject to the corporate security policy, and therefore are not high-risk computers. Computers on the network that are at the enterprise's remote offices, perhaps with different IS and security employees who have different ideas about security, are more risky than choices A and B, but obviously less risky than home computers.

NEW QUESTION 418

- (Topic 6)

The security level of a private key system depends on the number of:

- A. encryption key bit
- B. messages sent
- C. key
- D. channels used

Answer: A

Explanation:

The security level of a private key system depends on the number of encryption key bits. The larger the number of bits, the more difficult it would be to understand or determine the algorithm. The security of the message will depend on the encryption key bits used. More than keys by themselves, the algorithm and its complexity make the content more secured. Channels, which could be open or secure, are the mode for sending the message.

NEW QUESTION 423

- (Topic 6)

Which of the following manages the digital certificate life cycle to ensure adequate security and controls exist in digital signature applications related to e-commerce?

- A. Registration authority
- B. Certificate authority (CA)
- C. Certification relocation list
- D. Certification practice statement

Answer: B

Explanation:

The certificate authority maintains a directory of digital certificates for the reference of those receiving them, it manages the certificate life cycle, including certificate directory maintenance and certificate revocation list maintenance and publication. Choice A is not correct because a registration authority is an optional entity that is responsible for the administrative tasks associated with registering the end entity that is the subject of the certificate issued by the CA. Choice C is incorrect since a CRL is an instrument for checking the continued validity of the certificates for which the CA has responsibility. Choice D is incorrect because a certification practice statement is a detailed set of rules governing the certificate authority's operations.

NEW QUESTION 426

- (Topic 6)

An IS auditor doing penetration testing during an audit of internet connections would:

- A. evaluate configuration
- B. examine security settings
- C. ensure virus-scanning software is in use
- D. use tools and techniques available to a hacker

Answer: D

Explanation:

Penetration testing is a technique used to mimic an experienced hacker attacking a live site by using tools and techniques available to a hacker. The other choices are procedures that an IS auditor would consider undertaking during an audit of Internet connections, but are not aspects of penetration testing techniques.

NEW QUESTION 427

- (Topic 6)

During an audit of a telecommunications system, an IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST

effective control for reducing this exposure is:

- A. encryptio
- B. callback modem
- C. message authenticatio
- D. dedicated leased line

Answer: A

Explanation:

Encryption of data is the most secure method. The other methods are less secure, with leased lines being possibly the least secure method.

NEW QUESTION 431

- (Topic 6)

During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used when receiving communications from customers. To substantiate this, an IS auditor must prove that which of the following is used?

- A. A biometric, digitalized and encrypted parameter with the customer's public key
- B. A hash of the data that is transmitted and encrypted with the customer's private key
- C. A hash of the data that is transmitted and encrypted with the customer's public key
- D. The customer's scanned signature encrypted with the customer's public key

Answer: B

Explanation:

The calculation of a hash, or digest, of the data that are transmitted and its encryption require the public key of the client (receiver) and is called a signature of the message, or digital signature. The receiver performs the same process and then compares the received hash, once it has been decrypted with their private key, to the hash that is calculated with the received data. If they are the same, the conclusion would be that there is integrity in the data that have arrived and the origin is authenticated. The concept of encrypting the hash with the private key of the originator provides non repudiation, as it can only be decrypted with their public key and, as the CD suggests, the private key would not be known to the recipient. Simply put, in a key-pair situation, anything that can be decrypted by a sender's public key must have been encrypted with their private key, so they must have been the sender, i.e., non repudiation. Choice C is incorrect because, if this were the case, the hash could not be decrypted by the recipient, so the benefit of non repudiation would be lost and there could be no verification that the message had not been intercepted and amended. A digital signature is created by encrypting with a private key. A person creating the signature uses their own private key, otherwise everyone would be able to create a signature with any public key. Therefore, the signature of the client is created with the client's private key, and this can be verified-by

NEW QUESTION 434

- (Topic 6)

Which of the following is the MOST secure and economical method for connecting a private network over the Internet in a small- to medium-sized organization?

- A. Virtual private network
- B. Dedicated line
- C. Leased line
- D. integrated services digital network

Answer: A

Explanation:

The most secure method is a virtual private network (VPN), using encryption, authentication and tunneling to allow data to travel securely from a private network to the internet. Choices B, C and D are network connectivity options that are normally too expensive to be practical for small- to medium-sized organizations.

NEW QUESTION 439

- (Topic 6)

Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the internet?

- A. Transport mode with authentication header (AH) plus encapsulating security payload (ESP)
- B. Secure Sockets Layer (SSL) mode
- C. Tunnel mode with AH plus ESP
- D. Triple-DES encryption mode

Answer: C

Explanation:

Tunnel mode provides protection to the entire IP package. To accomplish this, AH and ESP services can be nested. The transport mode provides primary protection for the higher layers of the protocols by extending protection to the data fields (payload) of an IP package. The SSL mode provides security to the higher communication layers (transport layer). The triple-DES encryption mode is an algorithm that provides confidentiality

NEW QUESTION 441

- (Topic 6)

If inadequate, which of the following would be the MOST likely contributor to a denial-of-service attack?

- A. Router configuration and rules
- B. Design of the internal network
- C. Updates to the router system software
- D. Audit testing and review techniques

Answer: A

Explanation:

Inadequate router configuration and rules would lead to an exposure to denial-of-service attacks. Choices B and C would be lesser contributors. Choice D is incorrect because audit testing and review techniques are applied after the fact.

NEW QUESTION 443

.....

Relate Links

100% Pass Your CISA Exam with Exambible Prep Materials

<https://www.exambible.com/CISA-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>