Isaca

Exam Questions CISA

Isaca CISA

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

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

Answer: D

Explanation:

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

NEW QUESTION 2
- (Topic 1)
Which of the following is a benefit of using callback devices?

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

Answer: A

Explanation:

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

NEW QUESTION 3
- (Topic 1)
The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

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

Answer: D

Explanation:

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

NEW QUESTION 4
- (Topic 1)
An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

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

Answer: D

Explanation:

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

NEW QUESTION 5
- (Topic 1)
To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:

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

Answer: A

Explanation:

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

NEW QUESTION 6
- (Topic 1)
Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

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

Answer: D

Explanation:

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

NEW QUESTION 7
- (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 8
- (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 9
- (Topic 1)
An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST costeffective test of the DRP?

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

Answer: B

Explanation:

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

NEW QUESTION 10
- (Topic 1)
How does the process of systems auditing benefit from using a risk-based approach to audit planning?

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

Answer: B

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

NEW QUESTION 10
- (Topic 1)
After an IS auditor has identified threats and potential impacts, the auditor should:

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

Answer: A

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

NEW QUESTION 14
- (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 19
- (Topic 1)
If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

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

Answer: C

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

NEW QUESTION 21
- (Topic 1)
What is the most common purpose of a virtual private network implementation?

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

Answer: A

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

NEW QUESTION 23
- (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)
How does the SSL network protocol provide confidentiality?

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

Answer: D

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

NEW QUESTION 30
- (Topic 1)
Which of the following is a good control for protecting confidential data residing on a PC?

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

Answer: C

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

NEW QUESTION 31
- (Topic 1)
Which of the following is a guiding best practice for implementing logical access controls?

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

Answer: B

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

NEW QUESTION 35
- (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 40
- (Topic 1)
Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

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

Answer: A

Explanation:

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

NEW QUESTION 45
- (Topic 1)
What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 48
- (Topic 1)
Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

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

Answer: A

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

NEW QUESTION 51
- (Topic 1)
Which of the following typically focuses on making alternative processes and resources available for transaction processing?

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

Answer: D

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

NEW QUESTION 54
- (Topic 1)
Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive
management, such as the _____. (fill-in-the-blank)

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

Answer: C

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

NEW QUESTION 55
- (Topic 1)
Library control software restricts source code to:

A. Read-only access
B. Write-only access
C. Full access
D. Read-write access

Answer: A

Explanation:
Library control software restricts source code to read-only access.

NEW QUESTION 60

- (Topic 1)
What is a reliable technique for estimating the scope and cost of a software-development project?

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

Answer: A

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

NEW QUESTION 64
- (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 69
- (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 71
- (Topic 1)
An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 73
- (Topic 1)
Parity bits are a control used to validate:

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

Answer: B

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

NEW QUESTION 78
- (Topic 1)
Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

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

Answer: B

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

NEW QUESTION 80
- (Topic 1)
If an IS auditor finds evidence of risk involved in not implementing proper segregation of
duties, such as having the security administrator perform an operations function, what is the auditor's primary responsibility?

A. To advise senior managemen
B. To reassign job functions to eliminate potential frau
C. To implement compensator control
D. Segregation of duties is an administrative control not considered by an IS audito

Answer: A

Explanation:
An IS auditor's primary responsibility is to advise senior management of the risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function.

NEW QUESTION 82
- (Topic 1)
Why does an IS auditor review an organization chart?

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

Answer: C

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

NEW QUESTION 84
- (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 86
- (Topic 1)
Who should be responsible for network security operations?

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

Answer: B

Explanation:
Security administrators are usually responsible for network security operations.

NEW QUESTION 88
- (Topic 1)
Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

A. True
B. False

Answer: A

Explanation:
Proper segregation of duties does not prohibit a quality-control administrator from also being responsible for change control and problem management.

NEW QUESTION 90
- (Topic 1)

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

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

Answer: D

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

NEW QUESTION 92
- (Topic 1)
In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

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

Answer: B

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

NEW QUESTION 97
- (Topic 1)
What is an effective control for granting temporary access to vendors and external support personnel? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 102
- (Topic 1)
What are trojan horse programs? Choose the BEST answer.

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

Answer: D

Explanation:
Trojan horse programs are a common form of Internet attack.

NEW QUESTION 107
- (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 112
- (Topic 1)
What should IS auditors always check when auditing password files?

A. That deleting password files is protected
B. That password files are encrypted

C. That password files are not accessible over the network
D. That password files are archived

Answer: B

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

NEW QUESTION 114
- (Topic 1)
An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 119
- (Topic 1)
What is an acceptable recovery mechanism for extremely time-sensitive transaction processing?

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

Answer: C

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

NEW QUESTION 121
- (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 124
- (Topic 1)
When should application controls be considered within the system-development process?

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

Answer: D

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

NEW QUESTION 128
- (Topic 1)
When should plans for testing for user acceptance be prepared? Choose the BEST answer.

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

Answer: A

Explanation:

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

NEW QUESTION 131
- (Topic 1)
After identifying potential security vulnerabilities, what should be the IS auditor's next step?

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

Answer: C

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

NEW QUESTION 135
- (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 136
- (Topic 1)
Whenever business processes have been re-engineered, the IS auditor attempts to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 138
- (Topic 1)
When should an application-level edit check to verify that availability of funds was completed at the electronic funds transfer (EFT) interface?

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

Answer: D

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

NEW QUESTION 141
- (Topic 2)
Which of the following is a benefit of a risk-based approach to audit planning? Audit:

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

Answer: D

Explanation:

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

NEW QUESTION 146
- (Topic 2)
The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

A. information assets are overprotecte
B. a basic level of protection is applied regardless of asset valu
C. appropriate levels of protection are applied to information asset
D. an equal proportion of resources are devoted to protecting all information asset

Answer: C

Explanation:

Full risk assessment determines the level of protection most appropriate to a given level of risk, while the baseline approach merely applies a standard set of protection regardless of risk. There is a cost advantage in not overprotecting information. However, an even bigger advantage is making sure that no information assets are over- or underprotected. The risk assessment approach will ensure an appropriate level of protection is applied, commensurate with the level of risk and asset value and, therefore, considering asset value. The baseline approach does not allow more resources to be directed toward the assets at greater risk, rather than equally directing resources to all assets.

NEW QUESTION 151
- (Topic 2)
An IS auditor is assigned to perform a postimplementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:

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

Answer: A

Explanation:

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

NEW QUESTION 156
- (Topic 2)
To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

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

Answer: C

Explanation:

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

NEW QUESTION 161
- (Topic 2)
During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

A. address audit objective
B. collect sufficient evidenc
C. specify appropriate test
D. minimize audit resource

Answer: A

Explanation:

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

NEW QUESTION 164
CORRECT TEXT - (Topic 2)
The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

A. Test data
B. Generalized audit software
C. Integrated test facility
D. Embedded audit module

Answer: B

NEW QUESTION 166
- (Topic 2)
When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

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

Answer: A

Explanation:

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

NEW QUESTION 168
- (Topic 2)
An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

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

Answer: A

Explanation:

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

NEW QUESTION 173
- (Topic 2)
Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

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

Answer: D

Explanation:

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

NEW QUESTION 174
- (Topic 2)
The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

A. comply with regulatory requirement
B. provide a basis for drawing reasonable conclusion
C. ensure complete audit coverag
D. perform the audit according to the defined scop

Answer: B

Explanation:

The scope of an IS audit is defined by its objectives. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them. Complying with regulatory requirements, ensuring coverage and the execution of audit are all relevant to an audit but are not the reason why sufficient and relevant evidence is required.

NEW QUESTION 179
- (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 responsibilit
B. elaborate on the significance of the finding and the risks of not correcting i

C. report the disagreement to the audit committee for resolutio
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 182
- (Topic 3)
Which of the following is a function of an IS steering committee?

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

Answer: C

Explanation:

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

NEW QUESTION 185
- (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 properl
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 vendo

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 186
- (Topic 3)
As an outcome of information security governance, strategic alignment provides:

A. security requirements driven by enterprise requirement
B. baseline security following best practice
C. institutionalized and commoditized solution
D. an understanding of risk exposur

Answer: A

Explanation:

Information security governance, when properly implemented, should provide four basic outcomes: strategic alignment, value delivery, risk management and performance measurement. Strategic alignment provides input for security requirements driven by enterprise requirements. Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. Risk management provides an understanding of risk exposure.

NEW QUESTION 189
- (Topic 3)
Which of the following is the MOST important element for the successful implementation of IT governance?

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

Answer: B

Explanation:

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

NEW QUESTION 194
- (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 authorit
B. are current, documented and readily available to the employe
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 195
- (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 productivit
B. reduce the opportunity for an employee to commit an improper or illegal ac
C. provide proper cross-training for another employe
D. eliminate the potential disruption caused when an employee takes vacation one day at a tim

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 198
- (Topic 3)
A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual'sexperience and:

A. length of service, since this will help ensure technical competenc
B. age, as training in audit techniques may be impractica
C. IS knowledge, since this will bring enhanced credibility to the audit functio
D. ability, as an IS auditor, to be independent of existing IS relationship

Answer: D

Explanation:

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

NEW QUESTION 201
- (Topic 3)
An IS auditor should be concerned when a telecommunication analyst:

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

Answer: A

Explanation:

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

NEW QUESTION 206
- (Topic 3)
Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

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

Answer: D

Explanation:

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

NEW QUESTION 211
- (Topic 3)
Which of the following reduces the potential impact of social engineering attacks?

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

Answer: C

Explanation:

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

NEW QUESTION 215
- (Topic 3)
Which of the following is normally a responsibility of the chief security officer (CSO)?

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

Answer: A

Explanation:

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

NEW QUESTION 218
- (Topic 3)
When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

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

Answer: B

Explanation:

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

NEW QUESTION 219
- (Topic 3)
The PRIMARY objective of an audit of IT security policies is to ensure that:

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

Answer:

B

Explanation:

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

NEW QUESTION 223
- (Topic 3)
The development of an IS security policy is ultimately the responsibility of the:

A. IS departmen
B. security committe
C. security administrato
D. board of director

Answer: D

Explanation:

Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed by the board of directors. The security administrator is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized.

NEW QUESTION 227
- (Topic 3)
Which of the following is the initial step in creating a firewall policy?

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

Answer: B

Explanation:

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

NEW QUESTION 231
- (Topic 3)
An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

A. report that the control is operating effectively since deactivation happens within the time frame stated in the IS polic
B. verify that user access rights have been granted on a need-to-have basi
C. recommend changes to the IS policy to ensure deactivation of user IDs upon terminatio
D. recommend that activity logs of terminated users be reviewed on a regular basi

Answer: C

Explanation:

Although a policy provides a reference for performing IS audit assignments, an IS auditor needs to review the adequacy and the appropriateness of the policy. If, in the opinion of the auditor, the time frame defined for deactivation is inappropriate,the auditor needs to communicate this to management and recommend changes to the policy. Though the deactivation happens as stated in the policy, it cannot be concluded that the control is effective. Best practice would require that the ID of a terminated user be deactivated immediately. Verifying that user access rights have been granted on a need-to-have basis is necessary when permissions are granted. Recommending that activity logs of terminated users be reviewed on a regular basis is a good practice, but not as effective as deactivation upon termination.

NEW QUESTION 232
- (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 233
- (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 jurisdictio
B. Having a provider abroad will cause excessive costs in future audit
C. The auditing process will be difficult because of the distanc
D. There could be different auditing norm

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 234
- (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 organizatio
B. Periodic renegotiation is specified in the outsourcing contrac
C. The outsourcing contract fails to cover every action required by the arrangemen
D. Similar activities are outsourced to more than one vendo

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 235
- (Topic 3)
While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern shouldbe that the:

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

Answer: A

Explanation:

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

NEW QUESTION 236
- (Topic 3)
An organization has outsourced its help desk activities. An IS auditor's GREATEST concern when reviewing the contract and associated service level agreement (SLA) between the organization and vendor should be the provisions for:

A. documentation of staff background check
B. independent audit reports or full audit acces
C. reporting the year-to-year incremental cost reduction
D. reporting staff turnover, development or trainin

Answer: B

Explanation:

When the functions of an IS department are outsourced, an IS auditor should ensure that a provision is made for independent audit reports that cover all essential areas, or that the outsourcer has full audit access. Although it is necessary to document the fact that background checks are performed, this is not as important as provisions for audits. Financial measures such as year-to-year incremental cost reductions are desirable to have in a service level agreement (SLA); however, cost reductions are not as important as the availability of independent audit reports or full audit access. An SLA might include human relationship measures such as

resource planning, staff turnover, development or training, but this is not as important as the requirements for independent reports or full audit access by the outsourcing organization.

NEW QUESTION 241
- (Topic 3)
The output of the risk management process is an input for making:

A. business plan
B. audit charter
C. security policy decision
D. software design decision

Answer: C

Explanation:

The risk management process is about making specific, security-related decisions, such as the level of acceptable risk. Choices A, B and D are not ultimate goals of the risk
management process.

NEW QUESTION 243
- (Topic 3)
To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

A. avoidanc
B. transferenc
C. mitigatio
D. acceptanc

Answer: C

Explanation:

Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.

NEW QUESTION 244
- (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 247
- (Topic 4)
Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

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

Answer: B

Explanation:

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

NEW QUESTION 250
- (Topic 4)

A manager of a project was not able to implement all audit recommendations by the target date. The IS auditor should:

A. recommend that the project be halted until the issues are resolve
B. recommend that compensating controls be implemente
C. evaluate risks associated with the unresolved issue
D. recommend that the project manager reallocate test resources to resolve the issue

Answer: C

Explanation:

It is important to evaluate what the exposure would be when audit recommendations have not been completed by the target date. Based on the evaluation, management can accordingly consider compensating controls, risk acceptance, etc. All other choicesmight be appropriate only after the risks have been assessed.

NEW QUESTION 255
- (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 willaffect 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 257
- (Topic 4)
Before implementing controls, management should FIRST ensure that the controls:

A. satisfy a requirement in addressing a risk issu
B. do not reduce productivit
C. are based on a cost-benefit analysi
D. are detective or correctiv

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 259
- (Topic 4)
Information for detecting unauthorized input from a terminal would be BEST provided by the:

A. console log printou
B. transaction journa
C. automated suspense file listin
D. user error repor

Answer: B

Explanation:

The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error
occurred, while the user error report would only list input that resulted in an edit error.

NEW QUESTION 261
- (Topic 4)
What control detects transmission errors by appending calculated bits onto the end of each segment of data?

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

Answer: C

Explanation:

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

NEW QUESTION 263
- (Topic 4)
Which of the following is the GREATEST risk when implementing a data warehouse?

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

Answer: B

Explanation:

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

NEW QUESTION 266
- (Topic 4)
The MAIN purpose of a transaction audit trail is to:

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

Answer: B

Explanation:

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

NEW QUESTION 269
- (Topic 4)
An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

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

Answer: A

Explanation:

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

NEW QUESTION 270
- (Topic 4)
During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

A. test the software for compatibility with existing hardwar
B. perform a gap analysi
C. review the licensing polic
D. ensure that the procedure had been approve

Answer: D

Explanation:

In the case of a deviation from the predefined procedures, an IS auditor should first ensure that the procedure followed for acquiring the software is consistent with the business objectives and has been approved by the appropriate authorities. The other choices are not the first actions an IS auditor should take. They are steps that may or may not be taken after determining that the procedure used to acquire the software had been approved.

NEW QUESTION 274

- (Topic 4)
Ideally, stress testing should be carried out in a:

A. test environment using test dat
B. production environment using live workload
C. test environment using live workload
D. production environment using test dat

Answer: C

Explanation:

Stress testing is carried out to ensure a system can cope with production workloads. A test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment (choices Band D), and if only test data is used, there is no certainty that the system was stress tested adequately.

NEW QUESTION 277
- (Topic 4)
Which of the following is a dynamic analysis tool for the purpose of testing software modules?

A. Black box test
B. Desk checking
C. Structured walkthrough
D. Design and code

Answer: A

Explanation:

A black box test is a dynamic analysis tool for testing software modules. During the testing of software modules a black box test works first in a cohesive manner as a single unit/entity consisting of numerous modules, and second with the user data that flows across software modules, in some cases, this even drives the software behavior. In choices B, C and D, the software (design or code) remains static and someone closely examines it by applying their mind, without actually activating the software. Therefore, these cannot be referred to as dynamic analysis tools.

NEW QUESTION 278
- (Topic 4)
The phases and deliverables of a system development life cycle (SDLC) project should be determined:

A. during the initial planning stages of the projec
B. after early planning has been completed, but before work has begu
C. throughout the work stages, based on risks and exposure
D. only after all risks and exposures have been identified and the IS auditor has recommended appropriate control

Answer: A

Explanation:

It is extremely important that the project be planned properly and that the specific phases and deliverables be identified during the early stages of the project.

NEW QUESTION 283
- (Topic 4)
An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

A. a backup server be available to run ETCS operations with up-to-date dat
B. a backup server be loaded with all the relevant software and dat
C. the systems staff of the organization be trained to handle any even
D. source code of the ETCS application be placed in escro

Answer: D

Explanation:

Whenever proprietary application software is purchased, the contract should provide for a source code agreement. This will ensure that the purchasing company will have the opportunity to modify the software should the vendor cease to be in business.Having a backup server with current data and staff training is critical but not as critical as ensuring the availability of the source code.

NEW QUESTION 285
- (Topic 4)
Functionality is a characteristic associated with evaluating the quality of software products throughout their life cycle, and is BEST described as the set of attributes that bear on the:

A. existence of a set of functions and their specified propertie
B. ability of the software to be transferred from one environment to anothe
C. capability of software to maintain its level of performance under stated condition
D. relationship between the performance of the software and the amount of resources use

Answer: A

Explanation:

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

NEW QUESTION 287
- (Topic 4)
An IS auditor reviewing a proposed application software acquisition should ensure that the:

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

Answer: D

Explanation:

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

NEW QUESTION 290
- (Topic 4)
Which testing approach is MOST appropriate to ensure that internal application interface errors are identified as soon as possible?

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

Answer: C

Explanation:

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

NEW QUESTION 295
- (Topic 4)
During the requirements definition phase of a software development project, the aspects of software testing that should be addressed are developing:

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

Answer: D

Explanation:

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

NEW QUESTION 296
- (Topic 4)
Which of the following is an advantage of the top-down approach to software testing?

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

Answer: A

Explanation:

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

NEW QUESTION 297
- (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 299
- (Topic 4)
Which of the following types of testing would determine whether a new or modified system can operate in its target environment without adversely impacting other existing systems?

A. Parallel testing
B. Pilot testing
C. Interface/integration testing
D. Sociability testing

Answer: D

Explanation:

The purpose of sociability testing is to confirm that a new or modified system can operate in its target environment without adversely impacting existing systems. This should cover the platform that will perform primary application processing and interfaces with other systems, as well as changes to the desktop in a client-server or web development. Parallel testing is the process of feeding data into two systems-the modified system and an alternate system-and comparing the results. In this approach, the old and new systems operate concurrently for a period of time and perform the same processing functions. Pilot testing takes place first at one location and is then extended to other locations. The purpose is to see if the new system operates satisfactorily in one place before implementing it at other locations. Interface/integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another.The objective is to take unit-tested modules and build an integrated structure.

NEW QUESTION 303
- (Topic 4)
Which of the following would impair the independence of a quality assurance team?

A. Ensuring compliance with development methods
B. Checking the testing assumptions
C. Correcting coding errors during the testing process
D. Checking the code to ensure proper documentation

Answer: C

Explanation:

Correction of code should not be a responsibility of the quality assurance team as it would not ensure segregation of duties and would impair the team's independence. The other choices are valid quality assurance functions.

NEW QUESTION 305
- (Topic 4)
Responsibility and reporting lines cannot always be established when auditing automated systems since:

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

Answer: C

Explanation:

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

NEW QUESTION 308
- (Topic 4)
A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced?

A. Verifying production to customer orders
B. Logging all customer orders in the ERP system
C. Using hash totals in the order transmitting process
D. Approving (production supervisor) orders prior to production

Answer: A

Explanation:

Verification will ensure that production orders match customer orders. Logging can be used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processingcentrally. Production supervisory approval is a time consuming, manual process that does not guarantee proper control.

NEW QUESTION 313
- (Topic 4)
When two or more systems are integrated, input/output controls must be reviewed by an IS auditor in the:

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

Answer: C

Explanation:

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

NEW QUESTION 317
- (Topic 4)
The GREATEST advantage of using web services for the exchange of information between two systems is:

A. secure communication
B. improved performanc
C. efficient interfacin
D. enhanced documentatio

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 322
- (Topic 4)
When evaluating the controls of an EDI application, an IS auditor should PRIMARILY be concerned with the risk of:

A. excessive transaction turnaround tim
B. application interface failur
C. improper transaction authorizatio
D. nonvalidated batch total

Answer: C

Explanation:

Foremost among the risks associated with electronic data interchange (EDI) is improper transaction authorization. Since the interaction with the parties is electronic, there is no inherent authentication. The other choices, although risks, are not assignificant.

NEW QUESTION 327
- (Topic 4)
After discovering a security vulnerability in a third-party application that interfaces with several external systems, a patch is applied to a significant number of modules. Which of the following tests should an IS auditor recommend?

A. Stress
B. Black box
C. Interface
D. System

Answer: D

Explanation:

Given the extensiveness of the patch and its interfaces to external systems, system testing is most appropriate. Interface testing is not enough, and stress or black box testing are inadequate in these circumstances.

NEW QUESTION 332
- (Topic 5)
The PRIMARY objective of service-level management (SLM) is to:

A. define, agree, record and manage the required levels of servic

B. ensure that services are managed to deliver the highest achievable level of availabilit
C. keep the costs associated with any service at a minimu
D. monitor and report any legal noncompliance to business managemen

Answer: A

Explanation:

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

NEW QUESTION 334
- (Topic 5)
IT best practices for the availability and continuity of IT services should:

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

Answer: C

Explanation:

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

NEW QUESTION 336
- (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 338
- (Topic 5)
An IS auditor reviewing an organization's data file control procedures finds that transactions are applied to the most current files, while restart procedures use earlier versions. The IS auditor should recommend the implementation of:

A. source documentation retentio
B. data file securit
C. version usage contro
D. one-for-one checkin

Answer: C

Explanation:

For processing to be correct, it is essential that the proper version of a file is used. Transactions should be applied to the most current database, while restart procedures should use earlier versions. Source documentation should be retained for anadequate time period to enable documentation retrieval, reconstruction or verification of data, but it does not aid in ensuring that the correct version of a file will be used. Data file security controls prevent access by unauthorized users who could then alter the data files; however, it does not ensure that the correct file will be used. It is necessary to ensure that all documents have been received for processing, one-for-one; however, this does not ensure the use of the correct file.

NEW QUESTION 342
- (Topic 5)
Doing which of the following during peak production hours could result in unexpected downtime?

A. Performing data migration or tape backup
B. Performing preventive maintenance on electrical systems
C. Promoting applications from development to the staging environment

D. Replacing a failed power supply in the core router of the data center

Answer: B

Explanation:

Choices A and C are processing events which may impact performance, but would not cause downtime. Enterprise-class routers have redundant hot-swappable power supplies, so replacing a failed power supply should not be an issue. Preventive maintenanceactivities should be scheduled for non-peak times of the day, and preferably during a maintenance window time period. A mishap or incident caused by a maintenance worker could result in unplanned downtime.

NEW QUESTION 345
- (Topic 5)
The objective of concurrency control in a database system is to:

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

Answer: B

Explanation:

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

NEW QUESTION 349
- (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 reques
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 cannotbe 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 350
- (Topic 5)
An IS auditor finds that, at certain times of the day, the data warehouse query
performance decreases significantly. Which of the following controls would it be relevant for the IS auditor to review?

A. Permanent table-space allocation
B. Commitment and rollback controls
C. User spool and database limit controls
D. Read/write access log controls

Answer: C

Explanation:

User spool limits restrict the space available for running user queries. This prevents poorly formed queries from consuming excessive system resources and impacting general query performance. Limiting the space available to users in their own databases prevents them from building excessively large tables. This helps to control space utilization which itself acts to help performance by maintaining a buffer between the actual data volume stored and the physical device capacity. Additionally, it prevents users from consuming excessive resources in ad hoc table builds (as opposed to scheduled production loads that often can run overnight and are optimized for performance purposes), in a data warehouse, since you are not running online transactions, commitment and rollback does not have an impact on performance. The other choices are not as likely to be the root cause of this performance issue.

NEW QUESTION 353
- (Topic 5)
Which of the following types of firewalls provide the GREATEST degree and granularity of control?

A. Screening router
B. Packet filter
C. Application gateway
D. Circuit gateway

Answer: C

Explanation:

The application gateway is similar to a circuit gateway, but it has specific proxies for each service. To handle web services, it has an HTTP proxy that acts as an intermediary between externals and internals, but is specifically for HTTP. This meansthat it not only checks the packet IP addresses (layer 3) and the ports it is directed to (in this case port 80, or layer 4), it also checks every HTTP command (layers 5 and 7). Therefore, it works in a more detailed (granularity) way than the others. Screening router and packet filter (choices A and BJ work at the protocol, service and/or port level. This means that they analyze packets from layers 3 and 4, and not from higher levels. A circuit gateway (choice D) is based on a proxy or programthat acts as an intermediary between external and internal accesses. This means that during an external access, instead of opening a single connection to the internal server, two connections are established-one from the external server to the proxy(which conforms the circuit-gateway) and one from the proxy to the internal server. Layers 3 and 4 (IP and TCP) and some general features from higher protocols are used to perform these tasks.

NEW QUESTION 354
- (Topic 5)
In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

A. Automated logging of changes to development libraries
B. Additional staff to provide separation of duties
C. Procedures that verify that only approved program changes are implemented
D. Access controls to prevent the operator from making program modifications

Answer: C

Explanation:

While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited as suggested in choice B, this practice is not always possible in small organizations. An IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. An IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This would be a compensating control process. Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

NEW QUESTION 357
- (Topic 5)
Change management procedures are established by IS management to:

A. control the movement of applications from the test environment to the production environmen
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 disaste
D. verify that system changes are properly documente

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 358
- (Topic 5)
An organization has recently installed a security patch, which crashed the production server. To minimize the probability of this occurring again, an IS auditor should:

A. apply the patch according to the patch's release note
B. ensure that a good change management process is in plac
C. thoroughly test the patch before sending it to productio
D. approve the patch after doing a risk assessmen

Answer: B

Explanation:

An IS auditor must review the change management process, including patch management procedures, and verify that the process has adequate controls and make suggestions accordingly. The other choices are part of a good change management process but arenot an IS auditor's responsibility.

NEW QUESTION 360
- (Topic 5)
An IS auditor discovers that developers have operator access to the command line of a
production environment operating system. Which of the following controls wou Id BEST mitigate the risk of undetected and unauthorized program changes to the production
environment?

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

Answer: B

Explanation:

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

NEW QUESTION 364
- (Topic 5)
Time constraints and expanded needs have been found by an IS auditor to be the root causes for recent violations of corporate data definition standards in a new business intelligence project. Which of the following is the MOST appropriate suggestion for an auditor to make?

A. Achieve standards alignment through an increase of resources devoted to the project
B. Align the data definition standards after completion of the project
C. Delay the project until compliance with standards can be achieved
D. Enforce standard compliance by adopting punitive measures against violators

Answer: A

Explanation:

Provided that data architecture, technical, and operational requirements are sufficiently documented, the alignment to standards could be treated as a specific work package assigned to new project resources. The usage of nonstandard data definitionswould lower the efficiency of the new development, and increase the risk of errors in critical business decisions. To change data definition standards after project conclusion (choice B) is risky and is not a viable solution. On the other hand, punishing the violators (choice D) or delaying the project (choice C) would be an inappropriate suggestion because of the likely damage to the entire project profitability.

NEW QUESTION 366
- (Topic 5)
After installing a network, an organization installed a vulnerability assessment tool or security scanner to identify possible weaknesses. Which is the MOST serious risk associated with such tools?

A. Differential reporting
B. False-positive reporting
C. False-negative reporting
D. Less-detail reporting

Answer: C

Explanation:

False-negative reporting on weaknesses means the control weaknesses in the network are not identified and therefore may not be addressed, leaving the network vulnerable to attack. False-positive reporting is one in which the controls are in place, but are evaluated as weak, which should prompt a rechecking of the controls. Less-detail reporting and differential reporting functions provided by these tools compare scan results over a period of time.

NEW QUESTION 367
- (Topic 5)
The FIRST step in managing the risk of a cyber attack is to:

A. assess the vulnerability impac
B. evaluate the likelihood of threat
C. identify critical information asset
D. estimate potential damag

Answer: C

Explanation:

The first step in managing risk is the identification and classification of critical information resources (assets). Once the assets have been identified, the process moves onto the identification of threats, vulnerabilities and calculation of potential damages.

NEW QUESTION 369
- (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 vulnerabilit
B. Block the protocol traffic in the perimeter firewal
C. Block the protocol traffic between internal network segment
D. Stop the service until an appropriate security fix is installe

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 372
- (Topic 5)
The computer security incident response team (CSIRT) of an organization disseminates detailed descriptions of recent threats. An IS auditor's GREATEST concern should be that the users might:

A. use this information to launch attack
B. forward the security aler
C. implement individual solution
D. fail to understand the threa

Answer: A

Explanation:

An organization's computer security incident response team (CSIRT) should disseminate recent threats, security guidelines and security updates to the users to assist them in understanding the security risk of errors and omissions. However, this introduces the risk that the users may use this information to launch attacks, directly or indirectly. An IS auditor should ensure that the CSIRT is actively involved with users to assist them in mitigation of risks arising from security failures and to prevent additional security incidents resulting from the same threat. Forwarding the security alert is not harmful to the organization, implementing individual solutions is unlikely and users failing to understand the threat would not be a serious concern.

NEW QUESTION 375
- (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 377
- (Topic 5)
An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

A. Electromagnetic interference (EMI)
B. Cross-talk
C. Dispersion
D. Attenuation

Answer: D

Explanation:

Attenuation is the weakening of signals during transmission. When the signal becomes weak, it begins to read a 1 for a 0, and the user may experience communication problems. UTP faces attenuation around 100 meters. Electromagnetic interference (EMl)is caused by outside electromagnetic waves affecting the desired signals, which is not the case here. Cross-talk has nothing to do with the length of the UTP cable.

NEW QUESTION 379
- (Topic 5)
Which of the following line media would provide the BEST security for a telecommunication network?

A. Broadband network digital transmission
B. Baseband network
C. Dial-up
D. Dedicated lines

Answer: D

Explanation:

Dedicated lines are set apart for a particular user or organization. Since there is no sharing of lines or intermediate entry points, the risk of interception or disruption of telecommunications messages is lower.

NEW QUESTION 384
- (Topic 5)
Reconfiguring which of the following firewall types will prevent inward downloading of files through the File Transfer Protocol (FTP)?

A. Circuit gateway

B. Application gateway
C. Packet filter
D. Screening router

Answer: B

Explanation:

An application gateway firewall is effective in preventing applications, such as FTPs, from entering the organization network. A circuit gateway firewall is able to prevent paths or circuits, not applications, from entering the organization's network. A packet filter firewall or screening router will allow or prevent access based on IP packets/address.

NEW QUESTION 385
- (Topic 5)
Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?

A. Simple Network Management Protocol
B. File Transfer Protocol
C. Simple Mail Transfer Protocol
D. Telnet

Answer: A

Explanation:

The Simple Network Management Protocol provides a means to monitor and control network devices and to manage configurations and performance. The File Transfer Protocol (FTP) transfers files from a computer on the Internet to the user's computer and does not have any functionality related to monitoring network devices. Simple Mail Transfer Protocol (SMTP) is a protocol for sending and receiving e-mail messages and does not provide any monitoring or management for network devices. Telnet is a standard terminal emulation protocol used for remote terminal connections, enabling users to log into remote systems and use resources as if they were connected to a local system; it does not provide any monitoring or management of network devices.

NEW QUESTION 390
- (Topic 5)
An IS auditor examining the configuration of an operating system to verify the controls should review the:

A. transaction log
B. authorization table
C. parameter setting
D. routing table

Answer: C

Explanation:

Parameters allow a standard piece of software to be customized for diverse environments and are important in determining how a system runs. The parameter settings should be appropriate to an organization's workload and control environment, improper implementation and/or monitoring of operating systems can result in undetected errors and corruption of the data being processed, as well as lead to unauthorized access and inaccurate logging of system usage. Transaction logs are used to analyze transactions in master and/or transaction files. Authorization tables are used to verify implementation of logical access controls and will not be of much help when reviewing control features of an operating system. Routing tables do not contain information about the operating system and, therefore, provide no information to aid in the evaluation of controls.

NEW QUESTION 394
- (Topic 5)
Which significant risk is introduced by running the file transfer protocol (FTP) service on a server in a demilitarized zone (DMZ)?

A. A user from within could send a file to an unauthorized perso
B. FTP services could allow a user to download files from unauthorized source
C. A hacker may be able to use the FTP service to bypass the firewal
D. FTP could significantly reduce the performance of a DMZ serve

Answer: C

Explanation:

Since file transfer protocol (FTP) is considered an insecure protocol, it should not be installed on a server in a demilitarized zone (DMZ). FTP could allow an unauthorized user to gain access to the network. Sending files to an unauthorized person and the risk of downloading unauthorized files are not as significant as having a firewall breach. The presence of the utility does not reduce the performance of a DMZ server; therefore, performance degradation is not a threat.

NEW QUESTION 397
- (Topic 6)
Accountability for the maintenance of appropriate security measures over information assets resides with the:

A. security administrato
B. systems administrato
C. data and systems owner
D. systems operations grou

Answer: C

Explanation:

Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

NEW QUESTION 400
- (Topic 6)
Which of the following satisfies a two-factor user authentication?

A. Iris scanning plus fingerprint scanning
B. Terminal ID plus global positioning system (GPS)
C. A smart card requiring the user's PIN
D. User ID along with password

Answer: C

Explanation:

A smart card addresses what the user has. This is generally used in conjunction with testing what the user knows, e.g., a keyboard password or personal identification number (PIN). Proving who the user is usually requires a biometrics method, such as fingerprint, iris scan or voice verification, to prove biology. This is not a two-factor user authentication, because it proves only who the user is. A global positioning system (GPS) receiver reports on where the user is. The use of an ID and password (what the user knows) is a single-factor user authentication.

NEW QUESTION 405
- (Topic 6)
Which of the following exposures could be caused by a line grabbing technique?

A. Unauthorized data access
B. Excessive CPU cycle usage
C. Lockout of terminal polling
D. Multiplexor control dysfunction

Answer: A

Explanation:

Line grabbing will enable eavesdropping, thus allowing unauthorized data access, it will not necessarily cause multiplexor dysfunction, excessive CPU usage or lockout of terminal polling.

NEW QUESTION 406
- (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 aremonitored, captured, stored, processed and reported.

NEW QUESTION 408
- (Topic 6)
A hacker could obtain passwords without the use of computer tools or programs through the technique of:

A. social engineerin
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 maliciousin nature.

NEW QUESTION 411

- (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 lis
D. an inventory of IS resource

Answer: D

NEW QUESTION 416
- (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. Havingno 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 420
- (Topic 6)
An IS auditor reviewing digital rights management (DRM) applications should expect to find an extensive use for which of the following technologies?

A. Digitalized signatures
B. Hashing
C. Parsing
D. Steganography

Answer: D

Explanation:

Steganography is a technique for concealing the existence of messages or information. An increasingly important steganographical technique is digital watermarking, which hides data within data, e.g., by encoding rights information in a picture or music file without altering the picture or music's perceivable aesthetic qualities. Digitalized signatures are not related to digital rights management. Hashing creates a message hash or digest, which is used to ensure the integrity of the message; it is usually considered a part of cryptography. Parsing is the process of splitting up a continuous stream of characters for analytical purposes, and is widely applied in the design of programming languages or in data entry editing.

NEW QUESTION 423
- (Topic 6)
The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

A. Piggybacking
B. Shoulder surfing
C. Dumpster diving
D. Impersonation

Answer: A

Explanation:

Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger, if every employee must have theirbadge read at every controlled door no unauthorized person could enter the sensitive areA. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas using piggybacking,but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information. Some forms of social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

NEW QUESTION 426
- (Topic 6)
Which of the following BEST restricts users to those functions needed to perform their duties?

A. Application level access control
B. Data encryption
C. Disabling floppy disk drives
D. Network monitoring device

Answer: A

Explanation:

The use of application-level access control programs is a management control that restricts access by limiting users to only those functions needed to perform their duties. Data encryption and disabling floppy disk drives can restrict users to specific functions, but are not the best choices. A network monitoring device is a detective control, not a preventive control.

NEW QUESTION 428
- (Topic 6)
The logical exposure associated with the use of a checkpoint restart procedure is:

A. denial of servic
B. an asynchronous attac
C. wire tappin
D. computer shutdow

Answer: B

Explanation:

Asynchronous attacks are operating system-based attacks. A checkpoint restart is a feature that stops a program at specified intermediate points for later restart in an orderly manner without losing data at the checkpoint. The operating system savesa copy of the computer programs and data in their current state as well as several system parameters describing the mode and security level of the program at the time of stoppage. An asynchronous attack occurs when an individual with access to this information is able to gain access to the checkpoint restart copy of the system parameters and change those parameters such that upon restart the program would function at a higher-priority security level.

NEW QUESTION 431
- (Topic 6)
After reviewing its business processes, a large organization is deploying a new web application based on a VoIP technology. Which of the following is the MOST appropriate approach for implementing access control that will facilitate security management of the VoIP web application?

A. Fine-grained access control
B. Role-based access control (RBAC)
C. Access control lists
D. Network/service access control

Answer: B

Explanation:

Authorization in this VoIP case can best be addressed by role-based access control (RBAC) technology. RBAC is easy to manage and can enforce strong and efficient access controls in large-scale web environments including VoIP implementation. Access control lists and fine-grained access control on VoIP web applications do not scale to enterprisewide systems, because they are primarily based on individual user identities and their specific technical privileges. Network/service addresses VoIP availability but does not address application-level access or authorization.

NEW QUESTION 432
- (Topic 6)
In an online banking application, which of the following would BEST protect against identity theft?

A. Encryption of personal password
B. Restricting the user to a specific terminal
C. Two-factor authentication
D. Periodic review of access logs

Answer: C

Explanation:

Two-factor authentication requires two independent methods for establishing identity and privileges. Factors include something you know, such as a password; something you have, such as a token; and something you are, which is biometric. Requiring twoof these factors makes identity theft more difficult. A password could be guessed or broken. Restricting the user to a specific terminal is not a practical alternative for an online application. Periodic review of access logs is a detective controland does not protect against identity theft.

NEW QUESTION 437
- (Topic 6)
The responsibility for authorizing access to application data should be with the:

A. data custodia
B. database administrator (DBA).
C. data owne
D. security administrato

Answer: C

Explanation:

Data owners should have the authority and responsibility for granting access to the data and applications for which they are responsible. Data custodians are responsible only for storing and safeguarding the datA. The database administrator (DBA) isresponsible for managing the database and the security administrator is responsible for implementing and maintaining IS security. The ultimate responsibility for data resides with the data owner.

NEW QUESTION 441
- (Topic 6)
During an audit of the logical access control of an ERP financial system an IS auditor found some user accounts shared by multiple individuals. The user IDs were based on roles rather than individual identities. These accounts allow access to financial transactions on the ERP. What should the IS auditor do next?

A. Look for compensating control
B. Review financial transactions log
C. Review the scope of the audi
D. Ask the administrator to disable these account

Answer: A

Explanation:

The best logical access control practice is to create user IDs for each individual to define accountability. This is possible only by establishing a one-to-one relationship between IDs and individuals. However, if the user IDs are created based on role designations, an IS auditor should first understand the reasons and then evaluate the effectiveness and efficiency of compensating controls. Reviewing transactions logs is not relevant to an audit of logical access control nor is reviewing the scope of the audit relevant. Asking the administrator to disable the shared accounts should not be recommended by an IS auditor before understanding the reasons and evaluating the compensating controls. It is not an IS auditor's responsibility to ask for disabling accounts during an audit.

NEW QUESTION 445
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

* CISA Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year