Exam Questions CISA

Isaca CISA

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

NEW QUESTION 1
- (Topic 1)
A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

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

Answer: B

Explanation:

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

NEW QUESTION 2
- (Topic 1)
In an EDI process, the device which transmits and receives electronic documents is the:

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

Answer: A

Explanation:

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

NEW QUESTION 3
- (Topic 1)
Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

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

Answer: B

Explanation:

A compliance test determines if controls are operating as designed and are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned whether program library controls are working properly, the IS
auditor might select a sample of programs to determine if the source and object versions are the same. In other words, the broad objective of any compliance test is to provide auditors with reasonable assurance that a particular control on which the auditor plans to rely is operating as the auditor perceived it in the preliminary evaluation.

NEW QUESTION 4
- (Topic 1)
A malicious code that changes itself with each file it infects is called a:

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

Answer: D

Explanation:

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

NEW QUESTION 5
- (Topic 1)
Which of the following is a data validation edit and control?

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

Answer: B

Explanation:

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

NEW QUESTION 6
- (Topic 1)
What is the primary objective of a control self-assessment (CSA) program?

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

Answer: A

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

NEW QUESTION 7
- (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 8
- (Topic 1)
What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

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

Answer: B

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

NEW QUESTION 9
- (Topic 1)
Who is accountable for maintaining appropriate security measures over information assets?

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

Answer: A

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

NEW QUESTION 10
- (Topic 1)
Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 10
- (Topic 1)

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

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

Answer: D

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

NEW QUESTION 15
- (Topic 1)
What topology provides the greatest redundancy of routes and the greatest network fault tolerance?

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

Answer: B

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

NEW QUESTION 16
- (Topic 1)
What is an initial step in creating a proper firewall policy?

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

Answer: C

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

NEW QUESTION 21
- (Topic 1)
What are often the primary safeguards for systems software and data?

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

Answer: B

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

NEW QUESTION 24
- (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 27
- (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 31
- (Topic 1)
What is the key distinction between encryption and hashing algorithms?

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

Answer: B

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

NEW QUESTION 36
- (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 38
- (Topic 1)
The quality of the metadata produced from a data warehouse is _______________ in the warehouse's design. Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 41
- (Topic 1)
When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 46
- (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 51
- (Topic 1)
Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

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

Answer: D

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

NEW QUESTION 52
- (Topic 1)
If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 55
- (Topic 1)
Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures. True or false?

A. True
B. False

Answer: A

Explanation:
Fourth-generation languages(4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures.

NEW QUESTION 60
- (Topic 1)
Run-to-run totals can verify data through which stage(s) of application processing?

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

Answer: B

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

NEW QUESTION 65
- (Topic 1)
When storing data archives off-site, what must be done with the data to ensure data completeness?

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

Answer: D

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

NEW QUESTION 66
- (Topic 1)
A check digit is an effective edit check to:

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

Answer: B

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

NEW QUESTION 71
- (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 75
- (Topic 1)
What type of risk is associated with authorized program exits (trap doors)? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 77
- (Topic 1)
An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated datA. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 78
- (Topic 1)
An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 83
- (Topic 1)
When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 88
- (Topic 1)
When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

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

Answer: A

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

NEW QUESTION 92
- (Topic 1)
Allowing application programmers to directly patch or change code in production programs increases risk of fraud. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 94
- (Topic 1)
Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

A. Traffic analysis
B. SYN flood
C. Denial of service (DoS)
D. Distributed denial of service (DoS)

Answer: A

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

NEW QUESTION 95
- (Topic 1)
What is a callback system?

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

Answer: C

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

NEW QUESTION 98
- (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 101
- (Topic 1)
Which of the following provides the BEST single-factor authentication?

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

Answer: A

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

NEW QUESTION 106
- (Topic 1)
Which of the following is the most fundamental step in preventing virus attacks?

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

Answer: A

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

NEW QUESTION 108
- (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 110
- (Topic 1)
How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

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

Answer: B

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

NEW QUESTION 112
- (Topic 1)
Off-site data storage should be kept synchronized when preparing for recovery of time-sensitive data such as that resulting from which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 117
- (Topic 1)
Why is a clause for requiring source code escrow in an application vendor agreement important?

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

Answer: D

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

NEW QUESTION 121
- (Topic 1)
What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

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

Answer: C

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

NEW QUESTION 126
- (Topic 1)
Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

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

Answer: A

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

NEW QUESTION 127
- (Topic 1)
What is the primary security concern for EDI environments? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 131
- (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 135
- (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 137
- (Topic 1)
What is used as a control to detect loss, corruption, or duplication of data?

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

Answer: C

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

NEW QUESTION 141
- (Topic 2)
An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

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

Answer: C

Explanation:

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

NEW QUESTION 146
- (Topic 2)
The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

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

Answer: B

Explanation:

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

NEW QUESTION 147
- (Topic 2)
Which of the following is a substantive test?

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

Answer: C

Explanation:

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

NEW QUESTION 148
- (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 152
- (Topic 2)
Which of the following sampling methods is MOST useful when testing for compliance?

A. Attribute sampling
B. Variable sampling
C. Stratified mean per unit
D. Difference estimation

Answer: A

Explanation:

Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testingto confirm whether the quality exists. The other choices are used in substantive testing, which involves testing of details or quantity.

NEW QUESTION 153
- (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 155
- (Topic 2)
The PRIMARY purpose of an IT forensic audit is:

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

Answer: B

Explanation:

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

NEW QUESTION 160
- (Topic 2)
An IS auditor has imported data from the client's database. The next step-confirming whether the imported data are complete-is performed by:

A. matching control totals of the imported data to control totals of the original dat
B. sorting the data to confirm whether the data are in the same order as the original dat
C. reviewing the printout of the first 100 records of original data with the first 100 records of imported dat
D. filtering data for different categories and matching them to the original dat

Answer: A

Explanation:

Matching control totals of the imported data with control totals of the original data is the next logical step, as this confirms the completeness of the imported datA. It is not possible to confirm completeness by sorting the imported data, because the original data may not be in sorted order. Further, sorting does not provide control totals for verifying completeness. Reviewing a printout of 100 records of original data with 100 records of imported data is a process of physical verification andconfirms the accuracy of only these records. Filtering data for different categories and matching them to original data would still require that control totals be developed to confirm the completeness of the data.

NEW QUESTION 162
- (Topic 2)
During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

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

Answer: C

Explanation:

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

NEW QUESTION 163
- (Topic 2)
An integrated test facility is considered a useful audit tool because it:

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

Answer: C

Explanation:

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

NEW QUESTION 166
- (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 171
- (Topic 2)
An IS auditor evaluates the test results of a modification to a system that deals with payment computation. The auditor finds that 50 percent of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?

A. Design further tests of the calculations that are in erro
B. Identify variables that may have caused the test results to be inaccurat
C. Examine some of the test cases to confirm the result
D. Document the results and prepare a report of findings, conclusions and recommendation

Answer: C

Explanation:

An IS auditor should next examine cases where incorrect calculations occurred and confirm the results. After the calculations have been confirmed, further tests can be conducted and reviewed. Report preparation, findings and recommendations would notbe made until all results are confirmed.

NEW QUESTION 174
- (Topic 2)

The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs
B. recreating program logic using generalized audit software to calculate monthly total
C. preparing simulated transactions for processing and comparing the results to predetermined result
D. automatic flowcharting and analysis of the source code of the calculation program

Answer: C

Explanation:

Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

NEW QUESTION 175
- (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 177
- (Topic 2)
When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

A. analysi
B. evaluatio
C. preservatio
D. disclosur

Answer: C

Explanation:

Preservation and documentation of evidence for review by law enforcement and judicial authorities are of primary concern when conducting an investigation. Failure to properly preserve the evidence could jeopardize the acceptance of the evidence in legal proceedings. Analysis, evaluation and disclosure are important but not of primary concern in a forensic investigation.

NEW QUESTION 181
- (Topic 2)
The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

A. confirm that the auditors did not overlook any important issue
B. gain agreement on the finding
C. receive feedback on the adequacy of the audit procedure
D. test the structure of the final presentatio

Answer: B

Explanation:

The primary purpose for meeting with auditees prior to formally closing a review is to gain agreement on the findings. The other choices, though related to the formal closure of an audit, are of secondary importance.

NEW QUESTION 182
- (Topic 2)
Which of the following would an IS auditor use to determine if unauthorized modifications were made to production programs?

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

Answer: B

Explanation:

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

NEW QUESTION 183
- (Topic 2)
During a change control audit of a production system, an IS auditor finds that the change management process is not formally documented and that some migration procedures failed. What should the IS auditor do next?

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

Answer: B

Explanation:

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

NEW QUESTION 188
- (Topic 2)
An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

A. Personally delete all copies of the unauthorized softwar
B. Inform the auditee of the unauthorized software, and follow up to confirm deletio
C. Report the use of the unauthorized software and the need to prevent recurrence to auditee managemen
D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such us

Answer: C

Explanation:

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

NEW QUESTION 193
- (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 195
- (Topic 2)
A PRIMARY benefit derived from an organization employing control self-assessment (CSA) techniques is that it:

A. can identify high-risk areas that might need a detailed review late
B. allows IS auditors to independently assess ris
C. can be used as a replacement for traditional audit
D. allows management to relinquish responsibility for contro

Answer: A

Explanation:

CSA is predicated on the review of high-risk areas that either need immediate attention or a more thorough review at a later date. Choice B is incorrect, because CSA requires the involvement of auditors and line management. What occurs is that the internal audit function shifts some of the control monitoring responsibilities to the functional areas. Choice C is incorrect because CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them. Choice D is incorrect, because CSA does not allow management to relinquish its responsibility for control.

NEW QUESTION 198
- (Topic 3)
An IT steering committee should review information systems PRIMARILY to assess:

A. whether IT processes support business requirement
B. if proposed system functionality is adequat
C. the stability of existing softwar
D. the complexity of installed technolog

Answer: A

Explanation:

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

NEW QUESTION 200
- (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 204
- (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 208
- (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 212
- (Topic 3)
A local area network (LAN) administrator normally would be restricted from:

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

Answer: C

Explanation:

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

NEW QUESTION 216
- (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 217
- (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 220
- (Topic 3)
Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

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

Answer: A

Explanation:

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

NEW QUESTION 224
- (Topic 3)
To support an organization's goals, an IS department should have:

A. a low-cost philosoph
B. long- and short-range plan
C. leading-edge technolog
D. plans to acquire new hardware and softwar

Answer: B

Explanation:

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

NEW QUESTION 229
- (Topic 3)
An IS auditor reviewing an organization's IT strategic plan should FIRST review:

A. the existing IT environmen
B. the business pla
C. the present IT budge
D. current technology trend

Answer: B

Explanation:

The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the business plan.

NEW QUESTION 232
- (Topic 3)
To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

A. control self-assessment
B. a business impact analysi
C. an IT balanced scorecar
D. business process reengineerin

Answer: C

Explanation:

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

NEW QUESTION 234
- (Topic 3)
When reviewing an organization's strategic IT plan an IS auditor should expect to find:

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

Answer: A

Explanation:

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

NEW QUESTION 239
- (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 242
- (Topic 3)
Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

A. Time zone differences could impede communications between IT team
B. Telecommunications cost could be much higher in the first yea
C. Privacy laws could prevent cross-border flow of informatio
D. Software development may require more detailed specification

Answer: C

Explanation:

Privacy laws prohibiting the cross-border flow of personally identifiable information would make it impossible to locate a data warehouse containing customer information in another country. Time zone differences and higher telecommunications costs are more manageable. Software development typically requires more detailed specifications when dealing with offshore operations.

NEW QUESTION 244
- (Topic 3)
The initial step in establishing an information security program is the:

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

Answer: C

Explanation:

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

NEW QUESTION 248
- (Topic 3)
Which of the following provides the best evidence of the adequacy of a security awareness program?

A. The number of stakeholders including employees trained at various levels
B. Coverage of training at all locations across the enterprise
C. The implementation of security devices from different vendors
D. Periodic reviews and comparison with best practices

Answer: D

Explanation:

The adequacy of security awareness content can best be assessed by determining whether it is periodically reviewed and compared to industry best practices. Choices A, B and C provide metrics for measuring various aspects of a security awareness program, but do not help assess the content.

NEW QUESTION 252
- (Topic 3)
An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:

A. hardware configuratio
B. access control softwar
C. ownership of intellectual propert
D. application development methodolog

Answer: C

Explanation:

Of the choices, the hardware and access control software is generally irrelevant as long as the functionality, availability and security can be affected, which are specific contractual obligations. Similarly, the development methodology should be ofno real concern. The contract must, however, specify who owns the intellectual property (i.e., information being processed, application programs). Ownership of intellectual property will have a significant cost and is a key aspect to be defined in an outsourcing contract.

NEW QUESTION 257
- (Topic 3)
To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

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

Answer: B

Explanation:

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

NEW QUESTION 261

- (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 262
- (Topic 3)
An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

A. Report the risks to the CIO and CEO immediately
B. Examine e-business application in development
C. Identify threats and likelihood of occurrence
D. Check the budget available for risk management

Answer: C

Explanation:

An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

NEW QUESTION 263
- (Topic 3)
A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:

A. compute the amortization of the related asset
B. calculate a return on investment (ROI).
C. apply a qualitative approac
D. spend the time needed to define exactly the loss amoun

Answer: C

Explanation:

The common practice, when it is difficult to calculate the financial losses, is to take a qualitative approach, in which the manager affected by the risk defines the financial loss in terms of a weighted factor {e.g., one is a very low impact to thebusiness and five is a very high impact). An ROI is computed when there is predictable savings or revenues that can be compared to the investment needed to realize the revenues. Amortization is used in a profit and loss statement, not in computing potential losses. Spending the time needed to define exactly the total amount is normally a wrong approach. If it has been difficult to estimate potential losses (e.g., losses derived from erosion of public image due to a hack attack), that situation is not likely to change, and at the end of the day, the result will be a not well-supported evaluation.

NEW QUESTION 267
- (Topic 3)
Assessing IT risks is BEST achieved by:

A. evaluating threats associated with existing IT assets and IT project
B. using the firm's past actual loss experience to determine current exposur
C. reviewing published loss statistics from comparable organization
D. reviewing IT control weaknesses identified in audit report

Answer: A

Explanation:

To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves are not sufficient.Basing an assessment on past losses will not adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to beassessed. Comparable organizations will have differences in their IT assets, control environment and strategic circumstances. Therefore, their loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not all of the critical IT assets and projects will have recently been audited, and there may not be a sufficient assessment of strategic IT risks.

NEW QUESTION 269

- (Topic 4)
When auditing the proposed acquisition of a new computer system, an IS auditor should FIRST establish that:

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

Answer: A

Explanation:

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

NEW QUESTION 274
- (Topic 4)
The reason for establishing a stop or freezing point on the design of a new system is to:

A. prevent further changes to a project in proces
B. indicate the point at which the design is to be complete
C. require that changes after that point be evaluated for cost-effectivenes
D. provide the project management team with more control over the project desig

Answer: C

Explanation:

Projects often have a tendency to expand, especially during the requirements definition phase. This expansion often grows to a point where the originally anticipated cost-benefits are diminished because the cost of the project has increased. When this occurs, it is recommended that the project be stopped or frozen to allow a review of all of the cost-benefits and the payback period.

NEW QUESTION 277
- (Topic 4)
An IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could an IS auditor use to estimate the size of the development effort?

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

Answer: C

Explanation:

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

NEW QUESTION 278
- (Topic 4)
Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

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

Answer: B

Explanation:

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

NEW QUESTION 281
- (Topic 4)
An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. Of the following, who is PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

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

Answer: C

Explanation:

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

NEW QUESTION 285
- (Topic 4)
A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

A. what amount of progress against schedule has been achieve
B. if the project budget can be reduce
C. if the project could be brought in ahead of schedul
D. if the budget savings can be applied to increase the project scop

Answer: A

Explanation:

Cost performance of a project cannot be properly assessed in isolation of schedule performance. Cost cannot be assessed simply in terms of elapsed time on a project. To properly assess the project budget position it is necessary to know how much progress has actually been made and, given this, what level of expenditure would be expected. It is possible that project expenditure appears to be low because actual progress has been slow. Until the analysis of project against schedule has been completed, it is impossible to know whether there is any reason to reduce budget, if the project has slipped behind schedule, then not only may there be no spare budget but it is possible that extra expenditure may be needed to retrieve the slippage. The low expenditure could actually be representative of a situation where the project is likely to miss deadlines rather than potentially come in ahead of time. If the project is found to be ahead of budget after adjusting for actual progress, this is notnecessarily a good outcome because it points to flaws in the original budgeting process; and, as said above, until further analysis is undertaken, it cannot be determined whether any spare funds actually exist. Further, if the project is behind schedule, then adding scope may be the wrong thing to do.

NEW QUESTION 286
- (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 289
- (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 292
- (Topic 4)

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

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

Answer: C

Explanation:

A completeness check is used to determine if a field contains data and not zeros or blanks. A check digit is a digit calculated mathematically to ensure original data were not altered. An existence check also checks entered data for agreement to predetermined criteriA. A reasonableness check matches input to predetermined reasonable limits or occurrence rates.

NEW QUESTION 296
- (Topic 4)
Which of the following is the GREATEST risk to the effectiveness of application system controls?

A. Removal of manual processing steps
B. inadequate procedure manuals
C. Collusion between employees
D. Unresolved regulatory compliance issues

Answer: C

Explanation:

Collusion is an active attack that can be sustained and is difficult to identify since even well-thought-out application controls may be circumvented. The other choices do not impact well-designed application controls.

NEW QUESTION 297
- (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 300
- (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 302
- (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 304
- (Topic 4)
Which of the following is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality?

A. Function point analysis
B. Critical path methodology
C. Rapid application development
D. Program evaluation review technique

Answer: C

Explanation:

Rapid application development is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality. The program evaluation review technique (PERT) and critical path methodology (CPM) are both planning and control techniques, while function point analysis is used for estimating the complexity of developing business applications.

NEW QUESTION 308
- (Topic 4)
The reason a certification and accreditation process is performed on critical systems is to ensure that:

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

Answer: A

Explanation:

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

NEW QUESTION 309
- (Topic 4)
Which of the following would help to ensure the portability of an application connected to a database?

A. Verification of database import and export procedures
B. Usage of a structured query language (SQL)
C. Analysis of stored procedures/triggers
D. Synchronization of the entity-relation model with the database physical schema

Answer: B

Explanation:

The use of SQL facilitates portability. Verification of import and export procedures with other systems ensures better interfacing with other systems, analyzing stored procedures/triggers ensures proper access/performance, and reviewing the design entity-relation model will be helpful, but none of these contribute to the portability of an application connecting to a database.

NEW QUESTION 313
- (Topic 4)
A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following would be an IS auditor's main concern about the new process?

A. Whether key controls are in place to protect assets and information resources
B. If the system addresses corporate customer requirements
C. Whether the system can meet the performance goals (time and resources)
D. Whether owners have been identified who will be responsible for the process

Answer: A

Explanation:

The audit team must advocate the inclusion of the key controls and verify that the controls are in place before implementing the new process. Choices B, C and D are objectives that the business process reengineering (BPR) process should achieve, butthey are not the auditor's primary concern.

NEW QUESTION 315
- (Topic 4)
A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

A. Key verification
B. One-for-one checking

C. Manual recalculations
D. Functional acknowledgements

Answer: D

Explanation:

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

NEW QUESTION 320
- (Topic 4)
Which of the following represents the GREATEST potential risk in an EDI environment?

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

Answer: A

Explanation:

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

NEW QUESTION 325
- (Topic 4)
Which of the following is the MOST critical and contributes the greatest to the quality of data in a data warehouse?

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

Answer: A

Explanation:

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

NEW QUESTION 329
- (Topic 4)
An IS auditor reviewing an accounts payable system discovers that audit logs are not being reviewed. When this issue is raised with management the response is that additional controls are not necessary because effective system access controls are inplace. The BEST response the auditor can make is to:

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

Answer: C

Explanation:

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

NEW QUESTION 331
- (Topic 4)
A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not performing adequately which of the following types of testing?

A. Unit testing
B. Integration testing
C. Design walkthroughs
D. Configuration management

Answer: B

Explanation:

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

NEW QUESTION 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 335
- (Topic 5)
During a human resources (HR) audit, an IS auditor is informed that there is a verbal agreement between the IT and HR departments as to the level of IT services expected. In this situation, what should the IS auditor do FIRST?

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

Answer: C

Explanation:

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

NEW QUESTION 338
- (Topic 5)
Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

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

Answer: B

Explanation:

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

NEW QUESTION 339
- (Topic 5)
Which of the following BEST ensures the integrity of a server's operating system?

A. Protecting the server in a secure location
B. Setting a boot password
C. Hardening the server configuration
D. Implementing activity logging

Answer: C

Explanation:

Hardening a system means to configure it in the most secure manner (install latest security patches, properly define the access authorization for users and administrators, disable insecure options and uninstall unused services) to prevent nonprivileged users from gaining the right to execute privileged instructions and thus take control of the entire machine, jeopardizing the OS's integrity. Protecting the server in a secure location and setting a boot password are good practices, but do not ensure that a user will not try to exploit logical vulnerabilities and compromise the OS. Activity logging has two weaknesses in this scenario-it is a detective control (not a preventive one), and the attacker who already gained privileged accesscan modify logs or disable them.

NEW QUESTION 341
- (Topic 5)
The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

A. loss of confidentialit
B. increased redundanc
C. unauthorized accesse
D. application malfunction

Answer: B

Explanation:

Normalization is a design or optimization process for a relational database (DB) that minimizes redundancy; therefore, denormalization would increase redundancy. Redundancy which is usually considered positive when it is a question of resource availability is negative in a database environment, since it demands additional and otherwise unnecessary data handling efforts. Denormalization is sometimes advisable for functional reasons. It should not cause loss of confidentiality, unauthorized accesses or application malfunctions.

NEW QUESTION 346
- (Topic 5)
An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the MOST effective compensating control for this weakness?

A. Staging and job set up
B. Supervisory review of logs
C. Regular back-up of tapes
D. Offsite storage of tapes

Answer: A

Explanation:

If the IS auditor finds that there are effective staging and job set up processes, this can be accepted as a compensating control. Choice B is a detective control while choices C and D are corrective controls, none of which would serve as good compensating controls.

NEW QUESTION 349
- (Topic 5)
To verify that the correct version of a data file was used for a production run, an IS auditor should review:

A. operator problem report
B. operator work schedule
C. system log
D. output distribution report

Answer: C

Explanation:

System logs are automated reports which identify most of the activities performed on the computer. Programs that analyze the system log have been developed to report on specifically defined items. The auditor can then carry out tests to ensure that the correct file version was used for a production run. Operator problem reports are used by operators to log computer operation problems. Operator work schedules are maintained to assist in human resources planning. Output distribution reports identify all application reports generated and their distribution.

NEW QUESTION 353
- (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 354
- (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 358
- (Topic 5)
In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

A. Foreign key
B. Primary key
C. Secondary key
D. Public key

Answer: A

Explanation:

In a relational database with referential integrity, the use of foreign keys would prevent events such as primary key changes and record deletions, resulting in orphaned relations within the database. It should not be possible to delete a row from acustomer table when the customer number (primary key) of that row is stored with live orders on the orders table (the foreign key to the customer table). A primary key works in one table, so it is not able to provide/ensure referential integrity by itself. Secondary keys that are not foreign keys are not subject to referential integrity checks. Public key is related to encryption and not linked in any way to referential integrity.

NEW QUESTION 359
- (Topic 5)
When performing a database review, an IS auditor notices that some tables in the database are not normalized. The IS auditor should next:

A. recommend that the database be normalize
B. review the conceptual data mode
C. review the stored procedure
D. review the justificatio

Answer: D

Explanation:

If the database is not normalized, the IS auditor should review the justification since, in some situations, denormalization is recommended for performance reasons. The IS auditor should not recommend normalizing the database until further investigation takes place. Reviewing the conceptual data model or the stored procedures will not provide information about normalization.

NEW QUESTION 364
- (Topic 5)
Which of the following is MOST directly affected by network performance monitoring tools?

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

Answer: B

Explanation:

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

NEW QUESTION 367
- (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 369
- (Topic 5)
An IS auditor reviewing a database application discovers that the current configuration does not match the originally designed structure. Which of the following should be the IS auditor's next action?

A. Analyze the need for the structural chang
B. Recommend restoration to the originally designed structur
C. Recommend the implementation of a change control proces
D. Determine if the modifications were properly approve

Answer: D

Explanation:

An IS auditor should first determine if the modifications were properly approved. Choices A, B and C are possible subsequent actions, should the IS auditor find that the structural modification had not been approved.

NEW QUESTION 374
- (Topic 5)
The purpose of code signing is to provide assurance that:

A. the software has not been subsequently modifie
B. the application can safely interface with another signed applicatio
C. the signer of the application is truste
D. the private key of the signer has not been compromise

Answer: A

Explanation:

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

NEW QUESTION 376
- (Topic 5)
An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if:

A. the setup is geographically disperse
B. the network servers are clustered in a sit
C. a hot site is ready for activatio
D. diverse routing is implemented for the networ

Answer: B

Explanation:

A clustered setup in one location makes the entire network vulnerable to natural disasters or other disruptive events. Dispersed geographical locations and diverse routing provide backup if a site has been destroyed. A hot site would also be a good alternative for a single point-of-failure site.

NEW QUESTION 379
- (Topic 5)
Which of the following is a control over component communication failure/errors?

A. Restricting operator access and maintaining audit trails
B. Monitoring and reviewing system engineering activity
C. Providing network redundancy
D. Establishing physical barriers to the data transmitted over the network

Answer: C

Explanation:

Redundancy by building some form of duplication into the network components, such as a link, router or switch to prevent loss, delays or data duplication is a control over component communication failure or error. Other related controls are loop/echochecks to detect line errors, parity checks, error correction codes and sequence checks. Choices A, B and D are communication network controls.

NEW QUESTION 383
- (Topic 5)
Which of the following types of firewalls would BEST protect a network from an internet attack?

A. Screened subnet firewall
B. Application filtering gateway
C. Packet filtering router
D. Circuit-level gateway

Answer: A

Explanation:

A screened subnet firewall would provide the best protection. The screening router can be a commercial router or a node with routing capabilities and the ability to allow or avoid traffic between nets or nodes based on addresses, ports, protocols, interfaces, etc. Application-level gateways are mediators between two entities that want to communicate, also known as proxy gateways. The application level (proxy) works at the application level, not just at a package level. The screening controls atthe package level, addresses and ports, but does not see the contents of the package. A packet filtering router examines the header of every packet or data traveling between the internet and the corporate network.

NEW QUESTION 387
- (Topic 5)
In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?

A. Virus attack
B. Performance degradation
C. Poor management controls
D. Vulnerability to external hackers

Answer: B

Explanation:

Hubs are internal devices that usually have no direct external connectivity, and thus are not prone to hackers. There are no known viruses that are specific to hub attacks. While this situation may be an indicator of poor management controls, choiceB is more likely when the practice of stacking hubs and creating more terminal connections is used.

NEW QUESTION 390
- (Topic 5)
An organization provides information to its supply chain partners and customers through
an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

A. A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewal
B. Firewall policies are updated on the basis of changing requirement
C. inbound traffic is blocked unless the traffic type and connections have been specifically permitte
D. The firewall is placed on top of the commercial operating system with all installation option

Answer: D

Explanation:

The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall platform itself. In most circumstances, when commercial firewalls are breached that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options available on the system further increases the risks of vulnerabilities and exploits. Using SSL for firewall administration (choice A) is important, because changes in user and supply chain partners' roles and profiles will be dynamic. Therefore, it is appropriate to maintain the firewall policies daily (choice B), and prudent to block all inbound traffic unless permitted (choice C).

NEW QUESTION 391
- (Topic 5)
In large corporate networks having supply partners across the globe, network traffic may continue to rise. The infrastructure components in such environments should be scalable. Which of the following firewall architectures limits future scalability?

A. Appliances
B. Operating system-based
C. Host-based
D. Demilitarized

Answer: A

Explanation:

The software for appliances is embedded into chips. Firmware-based firewall products cannot be moved to higher capacity servers. Firewall software that sits on an operating system can always be scalable due to its ability to enhance the power of servers. Host-based firewalls operate on top of the server operating system and are scalable. A demilitarized zone is a model of firewall implementation and is not a firewall architecture.

NEW QUESTION 394
- (Topic 5)
Which of the following types of transmission media provide the BEST security against unauthorized access?

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

Answer: C

Explanation:

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

NEW QUESTION 398
- (Topic 5)
When auditing a proxy-based firewall, an IS auditor should:

A. verify that the firewall is not dropping any forwarded packet
B. review Address Resolution Protocol (ARP) tables for appropriate mapping between media access control (MAC) and IP addresse
C. verify that the filters applied to services such as HTTP are effectiv
D. test whether routing information is forwarded by the firewal

Answer: C

Explanation:

A proxy-based firewall works as an intermediary (proxy) between the service or application and the client, it makes a connection with the client and opens a different connection with the server and, based on specific filters and rules, analyzes all the traffic between the two connections. Unlike a packet-filtering gateway, a proxy-based firewall does not forward any packets. Mapping between media access control (MAC) and IP addresses is a task for protocols such as Address Resolution Protocol/Reverse Address Resolution Protocol (ARP/RARP).

NEW QUESTION 400
- (Topic 5)
An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?

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

Answer: B

Explanation:

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

NEW QUESTION 402
- (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 406
- (Topic 5)
When reviewing an implementation of a VoIP system over a corporate WAN, an IS auditor should expect to find:

A. an integrated services digital network (ISDN) data lin
B. traffic engineerin
C. wired equivalent privacy (WEP) encryption of dat
D. analog phone terminal

Answer: B

Explanation:

To ensure that quality of service requirements are achieved, the Voice-over IP (VoIP) service over the wide area network (WAN) should be protected from packet losses, latency or jitter. To reach this objective, the network performance can be managedusing statistical techniques such as traffic engineering. The standard bandwidth of an integrated services digital network (ISDN) data link would not provide the quality of services required for corporate VoIP services. WEP is an encryption scheme related to wireless networking. The VoIP phones are usually connected to a corporate local area network (LAN) and are not analog.

NEW QUESTION 407
- (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 409
- (Topic 6)
Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?

A. System analysis
B. Authorization of access to data
C. Application programming
D. Data administration

Answer: B

Explanation:

The application owner is responsible for authorizing access to datA. Application development and programming are functions of the IS department. Similarly, system analysis should be performed by qualified persons in IS who have knowledge of IS and user requirements. Data administration is a specialized function related to database management systems and should be performed by qualified database administrators.

NEW QUESTION 414
- (Topic 6)
Which of the following is the MOST effective control when granting temporary access to vendors?

A. Vendor access corresponds to the service level agreement (SLA).
B. User accounts are created with expiration dates and are based on services provide
C. Administrator access is provided for a limited perio
D. User IDs are deleted when the work is complete

Answer: B

Explanation:

The most effective control is to ensure that the granting of temporary access is based on services to be provided and that there is an expiration date (hopefully automated) associated with each ID. The SLA may have a provision for providing access, but this is not a control; it would merely define the need for access. Vendors require access for a limited period during the time of service. However, it is important to ensure that the access during this period is monitored. Deleting these user I Dsafter the work is completed is necessary, but if not automated, the deletion could be overlooked.

NEW QUESTION 417
- (Topic 6)
An IS auditor conducting an access control review in a client-server environment discovers that all printing options are accessible by all users. In this situation, the IS auditor is MOST likely to conclude that:

A. exposure is greater, since information is available to unauthorized user
B. operating efficiency is enhanced, since anyone can print any report at any tim
C. operating procedures are more effective, since information is easily availabl
D. user friendliness and flexibility is facilitated, since there is a smooth flow of information among user

Answer: A

Explanation:

Information in all its forms needs to be protected from unauthorized access. Unrestricted access to the report option results in an exposure. Efficiency and effectiveness are not relevant factors in this situation. Greater control over reports will not be accomplished since reports need not be in a printed form only. Information could be transmitted outside as electronic files, because print options allow for printing in an electronic form as well.

NEW QUESTION 419
- (Topic 6)
Electromagnetic emissions from a terminal represent an exposure because they:

A. affect noise pollutio
B. disrupt processor function
C. produce dangerous levels of electric curren
D. can be detected and displaye

Answer: D

Explanation:

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

NEW QUESTION 424
- (Topic 6)
Which of the following provides the framework for designing and developing logical access controls?

A. Information systems security policy
B. Access control lists
C. Password management
D. System configuration files

Answer: A

Explanation:

The information systems security policy developed and approved by an organization's top management is the basis upon which logical access control is designed and developed. Access control lists, password management and systems configuration files aretools for implementing the access controls.

NEW QUESTION 429
- (Topic 6)
An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as:

A. critica
B. vita
C. sensitiv
D. noncritica

Answer: C

Explanation:

Sensitive functions are best described as those that can be performed manually at a tolerable cost for an extended period of time. Critical functions are those that cannot be performed unless they are replaced by identical capabilities and cannot bereplaced by manual methods. Vital functions refer to those that can be performed manually but only for a brief period of time; this is associated with lower costs of disruption than critical functions. Noncritical functions may be interrupted for anextended period of time at little or no cost to the company, and require little time or cost to restore.

NEW QUESTION 434
- (Topic 6)
An information security policy stating that 'the display of passwords must be masked or suppressed' addresses which of the following attack methods?

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

Answer: C

Explanation:

If a password is displayed on a monitor, any person nearby could look over the shoulder of the user to obtain the password. Piggybacking refers to unauthorized persons following, either physically or virtually, authorized persons into restricted areas. Masking the display of passwords would not prevent someone from tailgating an authorized person. This policy only refers to 'the display of passwords.' If the policy referred to 'the display and printing of passwords' thenit would address shoulder surfing and dumpster diving (looking through an organization's trash for valuable information), impersonation refers to someone acting as an employee in an attempt to retrieve desired information.

NEW QUESTION 438
- (Topic 6)
To ensure compliance with a security policy requiring that passwords be a combination of letters and numbers, an IS auditor should recommend that:

A. the company policy be change
B. passwords are periodically change
C. an automated password management tool be use
D. security awareness training is delivere

Answer: C

Explanation:

The use of an automated password management tool is a preventive control measure. The software would prevent repetition (semantic) and would enforce syntactic rules, thus making the passwords robust. It would also provide a method for ensuring frequent changes and would prevent the same user from reusing their old password for a designated period of time. Choices A, B and D do not enforce compliance.

NEW QUESTION 441
- (Topic 6)
An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:

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

Answer: B

Explanation:

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

NEW QUESTION 445
- (Topic 6)
An IS auditor examining a biometric user authentication system establishes the existence
of a control weakness that would allow an unauthorized individual to update the centralized database on the server that is used to store biometric templates. Ofthe following, which is the BEST control against this risk?

A. Kerberos
B. Vitality detection
C. Multimodal biometrics
D. Before-image/after-image logging

Answer: A

Explanation:

Kerberos is a network authentication protocol for client-server applications that can be used to restrict access to the database to authorized users. Choices B and C are incorrect because vitality detection and multimodal biometrics are controls against spoofing and mimicry attacks. Before-image/after-image logging of database transactions is a detective control, as opposed to Kerberos, which is a preventative control.

NEW QUESTION 448
- (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 449
- (Topic 6)
Which of the following is the BEST method for preventing the leakage of confidential information in a laptop computer?

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

Answer: A

Explanation:

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

NEW QUESTION 453
- (Topic 6)
An IS auditor finds that a DBA has read and write access to production datA. The IS auditor should:

A. accept the DBA access as a common practic
B. assess the controls relevant to the DBA functio
C. recommend the immediate revocation of the DBA access to production dat

D. review user access authorizations approved by the DB

Answer: B

Explanation:

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

NEW QUESTION 455

......