# Isaca

## Exam Questions CISA

Isaca CISA

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 2**
- (Topic 1)
As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

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

**Answer:** C

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

**NEW QUESTION 3**
- (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 4**
- (Topic 1)
What type of approach to the development of organizational policies is often driven by risk assessment?

A. Bottom-up
B. Top-down
C. Comprehensive
D. Integrated

**Answer:** B

**Explanation:**
A bottom-up approach to the development of organizational policies is often driven by risk assessment.

**NEW QUESTION 5**
- (Topic 1)
What should an IS auditor do if he or she observes that project-approval procedures do not exist?

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

**Answer:** D

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

**NEW QUESTION 6**
- (Topic 1)
An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

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

**Answer:** A

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

**NEW QUESTION 7**
- (Topic 1)
What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?

A. Nonconnection-oriented protocols
B. Connection-oriented protocols
C. Session-oriented protocols
D. Nonsession-oriented protocols

**Answer:** B

**Explanation:**
The transport layer of the TCP/IP protocol suite provides for connection-oriented protocols to ensure reliable communication.

**NEW QUESTION 8**
- (Topic 1)
Why does the IS auditor often review the system logs?

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

**Answer:** C

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

**NEW QUESTION 9**
- (Topic 1)
How is risk affected if users have direct access to a database at the system level?

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

**Answer:** B

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

**NEW QUESTION 10**
- (Topic 1)
What can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program? Choose the BEST answer.

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

**Answer:** B

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

**NEW QUESTION 10**
- (Topic 1)
What are used as the framework for developing logical access controls?

A. Information systems security policies
B. Organizational security policies
C. Access Control Lists (ACL)

D. Organizational charts for identifying roles and responsibilities

**Answer:** A

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

**NEW QUESTION 12**
- (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 16**
- (Topic 1)
What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off? Choose the BEST answer.

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

**Answer:** C

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

**NEW QUESTION 17**
- (Topic 1)
Which of the following is used to evaluate biometric access controls?

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

**Answer:** B

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

**NEW QUESTION 19**
- (Topic 1)
Who is ultimately responsible and accountable for reviewing user access to systems?

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

**Answer:** C

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

**NEW QUESTION 21**
- (Topic 1)
Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

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

**Answer:** A

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

**NEW QUESTION 24**
- (Topic 1)
What influences decisions regarding criticality of assets?

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

**Answer:** C

**Explanation:**
Criticality of assets is often influenced by the business criticality of the data to be protected and by the scope of the impact upon the organization as a whole. For example, the loss of a network backbone creates a much greater impact on the organization as a whole than the loss of data on a typical user's workstation.

**NEW QUESTION 26**
- (Topic 1)
Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

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

**Answer:** A

**Explanation:**
Of the three major types of off-site processing facilities (hot, warm, and cold), a cold site is characterized by at least providing for electricity and HVAC. A warm site improves upon this by providing for redundant equipment and software that can be made operational within a short time.

**NEW QUESTION 27**
- (Topic 1)
Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

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

**Answer:** A

**Explanation:**
A cold site is often an acceptable solution for preparing for recovery of noncritical systems and datA.

**NEW QUESTION 28**
- (Topic 1)
Library control software restricts source code to:

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

**Answer:** A

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

**NEW QUESTION 31**
- (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 36**

- (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 40**
- (Topic 1)
What often results in project scope creep when functional requirements are not defined as well as they could be?

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

**Answer:** A

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

**NEW QUESTION 42**
- (Topic 1)
_____ risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a _____ risk assessment is more appropriate. Fill in the blanks.

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

**Answer:** A

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

**NEW QUESTION 43**
- (Topic 1)
A transaction journal provides the information necessary for detecting unauthorized _____ (fill in the blank) from a terminal.

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

**Answer:** B

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

**NEW QUESTION 45**
- (Topic 1)
An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

A. True
B. False

**Answer:** B

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

**NEW QUESTION 48**
- (Topic 1)
When are benchmarking partners identified within the benchmarking process?

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

**Answer:** C

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

**NEW QUESTION 49**
- (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 50**
- (Topic 1)
Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

A. True
B. False

**Answer:** A

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

**NEW QUESTION 51**
- (Topic 1)
The directory system of a database-management system describes:

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

**Answer:** B

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

**NEW QUESTION 56**
- (Topic 1)
When reviewing print systems spooling, an IS auditor is MOST concerned with which of the following vulnerabilities?

A. The potential for unauthorized deletion of report copies
B. The potential for unauthorized modification of report copies
C. The potential for unauthorized printing of report copies
D. The potential for unauthorized editing of report copies

**Answer:** C

**Explanation:**
When reviewing print systems spooling, an IS auditor is most concerned with the potential for unauthorized printing of report copies.

**NEW QUESTION 61**
- (Topic 1)
Which of the following are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem? Choose the BEST answer.

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

**Answer:** B

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

**NEW QUESTION 62**

- (Topic 1)
What supports data transmission through split cable facilities or duplicate cable facilities?

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

**Answer:** A

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

**NEW QUESTION 66**
- (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 70**
- (Topic 1)
When should systems administrators first assess the impact of applications or systems patches?

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

**Answer:** B

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

**NEW QUESTION 74**
- (Topic 1)
What are intrusion-detection systems (IDS) primarily used for?

A. To identify AND prevent intrusion attempts to a network
B. To prevent intrusion attempts to a network
C. Forensic incident response
D. To identify intrusion attempts to a network

**Answer:** D

**Explanation:**
Intrusion-detection systems (IDS) are used to identify intrusion attempts on a network.

**NEW QUESTION 79**
- (Topic 1)
Mitigating the risk and impact of a disaster or business interruption usually takes priority over transference of risk to a third party such as an insurer. True or false?

A. True
B. False

**Answer:** A

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

**NEW QUESTION 81**
- (Topic 1)
What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?

A. Contrived data
B. Independently created data

C. Live data
D. Data from previous tests

**Answer:** D

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

**NEW QUESTION 86**
- (Topic 1)
An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to:

A. Meet business objectives
B. Enforce data security
C. Be culturally feasible
D. Be financially feasible

**Answer:** A

**Explanation:**
An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to meet business objectives.

**NEW QUESTION 91**
- (Topic 1)
What kind of testing should programmers perform following any changes to an application or system?

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

**Answer:** A

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

**NEW QUESTION 94**
- (Topic 1)
Who is responsible for the overall direction, costs, and timetables for systems-development projects?

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

**Answer:** B

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

**NEW QUESTION 98**
- (Topic 1)
After identifying potential security vulnerabilities, what should be the IS auditor's next step?

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

**Answer:** C

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

**NEW QUESTION 101**
- (Topic 1)
Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?

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

**Answer:** B

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

**NEW QUESTION 102**
- (Topic 1)
Business process re-engineering often results in _____ automation, which results in _____ number of people using technology. Fill in the blanks.

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

**Answer:** A

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

**NEW QUESTION 106**
- (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 109**
- (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 111**
- (Topic 2)
An audit charter should:

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 112**
- (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 113**
- (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 118**
- (Topic 2)
The PRIMARY purpose of audit trails is to:

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 122**
- (Topic 2)
An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

A. the controls already in plac
B. the effectiveness of the controls in plac
C. the mechanism for monitoring the risks related to the asset
D. the threats/vulnerabilities affecting the asset

**Answer:** D

**Explanation:**

One of the key factors to be considered while assessing the risks related to the use of various information systems is the threats and vulnerabilities affecting the assets. The risks related to the use of information assets should be evaluated in isolation from the installed controls. Similarly, the effectiveness of the controls should be considered during the risk mitigation stage and not during the risk assessment phase A mechanism to continuously monitor the risks related to assets should be put in place during the risk monitoring function that follows the risk assessment phase.

**NEW QUESTION 123**
- (Topic 2)
An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

A. Issue an audit finding
B. Seek an explanation from IS management
C. Review the classifications of data held on the server
D. Expand the sample of logs reviewed

**Answer:** D

**Explanation:**

Audit standards require that an IS auditor gather sufficient and appropriate audit evidence. The auditor has found a potential problem and now needs to determine if this is an isolated incident or a systematic control failure. At this stage it is too preliminary to issue an audit finding and seeking an explanation from management is advisable, but it would be better to gather additional evidence to properly evaluate the seriousness of the situation. A backup failure, which has not been established at this point, will be serious if it involves critical datA. However, the issue is not the importance of the data on the server, where a problem has been

detected, but whether a systematic control failure that impacts other servers exists.

**NEW QUESTION 128**
- (Topic 2)
An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

A. There are a number of external modems connected to the networ
B. Users can install software on their desktop
C. Network monitoring is very limite
D. Many user IDs have identical password

**Answer:** D

**Explanation:**

Exploitation of a known user ID and password requires minimal technical knowledge and exposes the network resources to exploitation. The technical barrier is low and the impact can be very high; therefore, the fact that many user IDs have identical passwords represents the greatest threat. External modems represent a security risk, but exploitation still depends on the use of a valid user account. While the impact of users installing software on their desktops can be high {for example, due to the installation of Trojans or key-logging programs), the likelihood is not high due to the level of technical knowledge required to successfully penetrate the network. Although network monitoring can be a useful detective control, it will only detectabuse of user accounts in special circumstances and is, therefore, not a first line of defense.

**NEW QUESTION 131**
- (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 132**
- (Topic 2)
Which of the following would normally be the MOST reliable evidence for an auditor?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 136**
- (Topic 2)
When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 140**
- (Topic 2)
Which of the following would be the BEST population to take a sample from when testing program changes?

A. Test library listings
B. Source program listings
C. Program change requests
D. Production library listings

**Answer:** D

**Explanation:**

The best source from which to draw any sample or test of system information is the automated system. The production libraries represent executables that are approved and authorized to process organizational datA. Source program listings would be timeintensive. Program change requests are the documents used to initiate change; there is no guarantee that the request has been completed for all changes. Test library listings do not represent the approved and authorized executables.

**NEW QUESTION 143**
- (Topic 2)
Which of the following forms of evidence for the auditor would be considered the MOST reliable?

A. An oral statement from the auditee
B. The results of a test performed by an IS auditor
C. An internally generated computer accounting report
D. A confirmation letter received from an outside source

**Answer:** D

**Explanation:**

Evidence obtained from outside sources is usually more reliable than that obtained from within the organization. Confirmation letters received from outside parties, such as those used to verify accounts receivable balances, are usually highly reliable. Testing performed by an auditor may not be reliable, if the auditor did not have a good understanding of the technical area under review.

**NEW QUESTION 145**
- (Topic 2)
An IS auditor reviews an organizational chart PRIMARILY for:

A. an understanding of workflow
B. investigating various communication channel
C. understanding the responsibilities and authority of individual
D. investigating the network connected to different employee

**Answer:** C

**Explanation:**

An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps an IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information aboutthe roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

**NEW QUESTION 149**
- (Topic 2)
An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

A. evaluate the record retention plans for off-premises storag
B. interview programmers about the procedures currently being followe
C. compare utilization records to operations schedule
D. review data file access records to test the librarian functio

**Answer:** B

**Explanation:**

Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests the recovery procedures, not the access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

**NEW QUESTION 154**
- (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 158**
- (Topic 2)
An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

A. conclude that the controls are inadequat
B. expand the scope to include substantive testin
C. place greater reliance on previous audit
D. suspend the audi

**Answer:** B

**Explanation:**

If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of testing the controls and include additional substantive tests. There is no evidence that whatever controls might exist are either inadequate or adequate. Placing greater reliance on previous audits or suspending the audit are inappropriate actions as they provide no current knowledge of the adequacy of the existing controls.

**NEW QUESTION 162**
- (Topic 2)
The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 166**
- (Topic 2)
In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

A. examine source program changes without information from IS personne
B. detect a source program change made between acquiring a copy of the source and the comparison ru
C. confirm that the control copy is the current version of the production progra
D. ensure that all changes made in the current source copy are detecte

**Answer:** A

**Explanation:**

An IS auditor has an objective, independent and relatively complete assurance of program changes because the source code comparison will identify changes. Choice B is incorrect, because the changes made since the acquisition of the copy are not included in the copy of the software. Choice C is incorrect, as an IS auditor will have to gain this assurance separately. Choice D is incorrect, because any changes made between the time the control copy was acquired and the source code comparison is made will not be detected.

**NEW QUESTION 170**
- (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 174**
- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 178**
- (Topic 2)
When preparing an audit report the IS auditor should ensure that the results are supported by:

A. statements from IS managemen
B. workpapers of other auditor
C. an organizational control self-assessmen
D. sufficient and appropriate audit evidenc

**Answer:** D

**Explanation:**

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

**NEW QUESTION 183**
- (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 185**
- (Topic 3)
The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

A. a lack of investment in technolog
B. a lack of a methodology for systems developmen
C. technology not aligning with the organization's objective
D. an absence of control over technology contract

**Answer:** C

**Explanation:**

A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

**NEW QUESTION 188**
- (Topic 3)
Which of the following IT governance best practices improves strategic alignment?

A. Supplier and partner risks are manage
B. A knowledge base on customers, products, markets and processes is in plac
C. A structure is provided that facilitates the creation and sharing of business informatio
D. Top management mediate between the imperatives of business and technolog

**Answer:** D

**Explanation:**

Top management mediating between the imperatives of business and technology is an IT strategic alignment best practice. Supplier and partner risks being managed is a risk management best practice. A knowledge base on customers, products, markets andprocesses being in place is an IT value delivery best practice. An infrastructure being provided to facilitate the creation and sharing of business information is an IT value delivery and risk management best practice.

**NEW QUESTION 193**
- (Topic 3)
What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 194**
- (Topic 3)
From a control perspective, the key element in job descriptions is that they:

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 195**
- (Topic 3)
An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 197**
- (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 202**

- (Topic 3)
Which of the following is a risk of cross-training?

A. Increases the dependence on one employee
B. Does not assist in succession planning
C. One employee may know all parts of a system
D. Does not help in achieving a continuity of operations

**Answer:** C

**Explanation:**

When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

**NEW QUESTION 204**
- (Topic 3)
Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

A. has been approved by line managemen
B. does not vary from the IS department's preliminary budge
C. complies with procurement procedure
D. supports the business objectives of the organizatio

**Answer:** D

**Explanation:**

Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals. Choice A is incorrectsince line management prepared the plans.

**NEW QUESTION 205**
- (Topic 3)
When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

A. establishment of a review boar
B. creation of a security uni
C. effective support of an executive sponso
D. selection of a security process owne

**Answer:** C

**Explanation:**

The executive sponsor would be in charge of supporting the organization's strategic security program, and would aid in directing the organization's overall security management activities. Therefore, support by the executive level of management is themost critical success factor (CSF). None of the other choices are effective without visible sponsorship of top management.

**NEW QUESTION 206**
- (Topic 3)
The PRIMARY objective of an audit of IT security policies is to ensure that:

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 211**
- (Topic 3)
An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

A. this lack of knowledge may lead to unintentional disclosure of sensitive informatio
B. information security is not critical to all function
C. IS audit should provide security training to the employee
D. the audit finding will cause management to provide continuous training to staf

**Answer:** A

**Explanation:**

All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

**NEW QUESTION 215**
- (Topic 3)
A retail outlet has introduced radio frequency identification (RFID) tags to create unique serial numbers for all products. Which of the following is the PRIMARY concern associated with this initiative?

A. Issues of privacy
B. Wavelength can be absorbed by the human body
C. RFID tags may not be removable
D. RFID eliminates line-of-sight reading

**Answer:** A

**Explanation:**

The purchaser of an item will not necessarily be aware of the presence of the tag. If a tagged item is paid for by credit card, it would be possible to tie the unique ID of that item to the identity of the purchaser. Privacy violations are a significant concern because RFID can carry unique identifier numbers. If desired it would be possible for a firm to track individuals who purchase an item containing an RFID. Choices B and C are concerns of less importance. Choice D is not a concern.

**NEW QUESTION 218**
- (Topic 3)
IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

A. desired result or purpose of implementing specific control procedure
B. best IT security control practices relevant to a specific entit
C. techniques for securing informatio
D. security polic

**Answer:** A

**Explanation:**

An IT control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. They provide the actual objectives for implementing controls and may or may not be the best practices. Techniques are the means of achieving an objective, and a security policy is a subset of IT control objectives.

**NEW QUESTION 220**
- (Topic 3)
The PRIMARY objective of implementing corporate governance by an organization's management is to:

A. provide strategic directio
B. control business operation
C. align IT with busines
D. implement best practice

**Answer:** A

**Explanation:**

Corporate governance is a set of management practices to provide strategic direction, thereby ensuring that goals are achievable, risks are properly addressed and organizational resources are properly utilized. Hence, the primary objective of corporate governance is to provide strategic direction. Based on the strategic direction, business operations are directed and controlled.

**NEW QUESTION 225**
- (Topic 3)
A benefit of open system architecture is that it:

A. facilitates interoperabilit
B. facilitates the integration of proprietary component
C. will be a basis for volume discounts from equipment vendor
D. allows for the achievement of more economies of scale for equipmen

**Answer:** A

**Explanation:**

Open systems are those for which suppliers provide components whose interfaces are
defined by public standards, thus facilitating interoperability between systems made by different vendors. In contrast, closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems.

**NEW QUESTION 230**
- (Topic 3)
Which of the following BEST supports the prioritization of new IT projects?

A. Internal control self-assessment (CSA)

B. Information systems audit
C. Investment portfolio analysis
D. Business risk assessment

**Answer:** C

**Explanation:**

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

**NEW QUESTION 235**
- (Topic 3)
When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 236**
- (Topic 3)
Which of the following is the BEST information source for management to use as an aid in the identification of assets that are subject to laws and regulations?

A. Security incident summaries
B. Vendor best practices
C. CERT coordination center
D. Significant contracts

**Answer:** D

**Explanation:**

Contractual requirements are one of the sources that should be consulted to identify the requirements for the management of information assets. Vendor best practices provides a basis for evaluating how competitive an enterprise is, while security incident summaries are a source for assessing the vulnerabilities associated with the IT infrastructure. CERT {www.cert.org) is an information source for assessing vulnerabilities within the IT infrastructure.

**NEW QUESTION 240**
- (Topic 3)
Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

A. meets or exceeds industry security standard
B. agrees to be subject to external security review
C. has a good market reputation for service and experienc
D. complies with security policies of the organizatio

**Answer:** B

**Explanation:**

It is critical that an independent security review of an outsourcing vendor be obtained because customer credit information will be kept there. Compliance with security standards or organization policies is important, but there is no way to verify orprove that that is the case without an independent review. Though long experience in business and good reputation is an important factor to assess service quality, the business cannot outsource to a provider whose security control is weak.

**NEW QUESTION 241**
- (Topic 3)
Which of the following should be considered FIRST when implementing a risk management program?

A. An understanding of the organization's threat, vulnerability and risk profile
B. An understanding of the risk exposures and the potential consequences of compromise
C. A determination of risk management priorities based on potential consequences
D. A risk mitigation strategy sufficient to keep risk consequences at an acceptable level

**Answer:** A

**Explanation:**

Implementing risk management, as one of the outcomes of effective information security governance, would require a collective understanding of the organization's threat, vulnerability and risk profile as a first step. Based on this, an understanding of risk exposure and potential consequences of compromise could be determined. Risk management priorities based on potential consequences could then be developed. This would provide a basis for the formulation of strategies for risk mitigation sufficient to keep the consequences from risk at an acceptable level.

**NEW QUESTION 245**
- (Topic 3)
The PRIMARY benefit of implementing a security program as part of a security governance framework is the:

A. alignment of the IT activities with IS audit recommendation
B. enforcement of the management of security risk
C. implementation of the chief information security officer's (CISO) recommendation
D. reduction of the cost for IT securit

**Answer:** B

**Explanation:**

The major benefit of implementing a security program is management's assessment of risk and its mitigation to an appropriate level of risk, and the monitoring of the remaining residual risks. Recommendations, visions and objectives of the auditor and the chief information security officer (CISO) are usually included within a security program, but they would not be the major benefit. The cost of IT security may or may not be reduced.

**NEW QUESTION 248**
- (Topic 3)
The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

A. financial result
B. customer satisfactio
C. internal process efficienc
D. innovation capacit

**Answer:** A

**Explanation:**

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

**NEW QUESTION 252**
- (Topic 3)
Before implementing an IT balanced scorecard, an organization must:

A. deliver effective and efficient service
B. define key performance indicator
C. provide business value to IT project
D. control IT expense

**Answer:** B

**Explanation:**

A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

**NEW QUESTION 257**
- (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 261**
- (Topic 4)
An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project

manager responds that it is too early to identify risks and that, if risks do start impactingthe project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 266**
- (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 268**
- (Topic 4)
The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

A. integrit
B. authenticit
C. authorizatio
D. nonrepudiatio

**Answer:** A

**Explanation:**

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

**NEW QUESTION 270**
- (Topic 4)
Information for detecting unauthorized input from a terminal would be BEST provided by the:

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 274**
- (Topic 4)
Functional acknowledgements are used:

A. as an audit trail for EDI transaction

B. to functionally describe the IS departmen
C. to document user roles and responsibilitie
D. as a functional description of application softwar

**Answer:** A

**Explanation:**

Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

**NEW QUESTION 276**
- (Topic 4)
Which of the following is the GREATEST risk when implementing a data warehouse?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 280**
- (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 281**
- (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 286**
- (Topic 4)
The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:

A. rule
B. decision tree
C. semantic net
D. dataflow diagram

**Answer:** B

**Explanation:**

Decision trees use questionnaires to lead a user through a series of choices until a conclusion is reached. Rules refer to the expression of declarative knowledge

through the use of if-then relationships. Semantic nets consist of a graph in which nodes represent physical or conceptual objects and the arcs describe the relationship between the nodes. Semantic nets resemble a dataflow diagram and make use of an inheritance mechanism to prevent duplication of data.

**NEW QUESTION 287**
- (Topic 4)
Which of the following should be included in a feasibility study for a project to implement an EDI process?

A. The encryption algorithm format
B. The detailed internal control procedures
C. The necessary communication protocols
D. The proposed trusted third-party agreement

**Answer:** C

**Explanation:**

Encryption algorithms, third-party agreements and internal control procedures are too detailed for this phase. They would only be outlined and any cost or performance implications shown. The communications protocols must be included, as there may besignificant cost implications if new hardware and software are involved, and risk implications if the technology is new to the organization.

**NEW QUESTION 289**
- (Topic 4)
An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 294**
- (Topic 4)
The GREATEST advantage of rapid application development (RAD) over the traditional system development life cycle (SDLC) is that it:

A. facilitates user involvemen
B. allows early testing of technical feature
C. facilitates conversion to the new syste
D. shortens the development time fram

**Answer:** D

**Explanation:**

The greatest advantage of RAD is the shorter time frame for the development of a system. Choices A and B are true, but they are also true for the traditional systems development life cycle. Choice C is not necessarily always true.

**NEW QUESTION 295**
- (Topic 4)
An IS auditor reviewing a proposed application software acquisition should ensure that the:

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 299**
- (Topic 4)
The waterfall life cycle model of software development is most appropriately used when:

A. requirements are well understood and are expected to remain stable, as is the business environment in which the system will operat
B. requirements are well understood and the project is subject to time pressure

C. the project intends to apply an object-oriented design and programming approac
D. the project will involve the use of new technolog

**Answer:** A

**Explanation:**

Historically, the waterfall model has been best suited to the stable conditions described in choice A. When the degree of uncertainty of the system to be delivered and the conditions in which it will be used rises, the waterfall model has not been successful, in these circumstances, the various forms of iterative development life cycle gives the advantage of breaking down the scope of the overall system to be delivered, making the requirements gathering and design activities more manageable. Theability to deliver working software earlier also acts to alleviate uncertainty and may allow an earlier realization of benefits. The choice of a design and programming approach is not itself a determining factor of the type of software development life cycle that is appropriate. The use of new technology in a project introduces a significant element of risk. An iterative form of development, particularly one of the agile methods that focuses on early development of actual working software, is likely to be the better option to manage this uncertainty.

**NEW QUESTION 303**
- (Topic 4)
Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

A. System owners
B. System users
C. System designers
D. System builders

**Answer:** A

**Explanation:**

System owners are the information systems (project) sponsors or chief advocates. They normally are responsible for initiating and funding projects to develop, operate and maintain information systems. System users are the individuals who use or are affected by the information system. Their requirements are crucial in the testing stage of a project. System designers translate business requirements and constraints into technical solutions. System builders construct the system based on the specifications from the systems designers. In most cases, the designers and builders are one and the same.

**NEW QUESTION 308**
- (Topic 4)
Which of the following types of testing would determine whether a new or modified system can operate in its target environment without adversely impacting other existing systems?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 310**
- (Topic 4)
An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?

A. Pilot
B. Parallel
C. Direct cutover
D. Phased

**Answer:** C

**Explanation:**

Direct cutover implies switching to the new system immediately, usually without the ability to revert to the old system in the event of problems. All other alternatives are done gradually and thus provide greater recoverability and are therefore less risky.

**NEW QUESTION 315**
- (Topic 4)
Which of the following system and data conversion strategies provides the GREATEST redundancy?

A. Direct cutover
B. Pilot study
C. Phased approach
D. Parallel run

**Answer:** D

**Explanation:**

Parallel runs are the safest-though the most expensive-approach, because both the old and new systems are run, thus incurring what might appear to be double costs. Direct cutover is actually quite risky, since it does not provide for a 'shake down period' nor does it provide an easy fallback option. Both a pilot study and a phased approach are
performedincrementally, making rollback procedures difficult to execute.

**NEW QUESTION 319**
- (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 321**
- (Topic 4)
Business units are concerned about the performance of a newly implemented system. Which of the following should an IS auditor recommend?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 325**
- (Topic 4)
An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:

A. EDI trading partner agreement
B. physical controls for terminal
C. authentication techniques for sending and receiving message
D. program change control procedure

**Answer:** C

**Explanation:**

Authentication techniques for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

**NEW QUESTION 327**
- (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 330**
- (Topic 4)

When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:

A. not be concerned since there may be other compensating controls to mitigate the risk
B. ensure that overrides are automatically logged and subject to revie
C. verify whether all such overrides are referred to senior management for approva
D. recommend that overrides not be permitte

**Answer:** B

**Explanation:**

If input procedures allow overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log. An IS auditor should not assume that compensating controls exist. Aslong as the overrides are policy-compliant, there is no need for senior management approval or a blanket prohibition.

**NEW QUESTION 334**
- (Topic 4)
When performing an audit of a client relationship management (CRM) system migration project, which of the following should be of GREATEST concern to an IS auditor?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 336**
- (Topic 5)
An organization has outsourced its help desk. Which of the following indicators would be the best to include in the SLA?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 337**
- (Topic 5)
Which of the following should be of PRIMARY concern to an IS auditor reviewing the management of external IT service providers?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 338**
- (Topic 5)
To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?

A. System access log files

B. Enabled access control software parameters
C. Logs of access control violations
D. System configuration files for control options used

**Answer:** D

**Explanation:**

A review of system configuration files for control options used would show which users have access to the privileged supervisory state. Both systems access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

**NEW QUESTION 340**
- (Topic 5)
Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance
program?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 343**
- (Topic 5)
Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?

A. Sensitive data can be read by operator
B. Data can be amended without authorizatio
C. Unauthorized report copies can be printe
D. Output can be lost in the event of system failur

**Answer:** C

**Explanation:**

Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operators. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure.

**NEW QUESTION 346**
- (Topic 5)
Which of the following is a network diagnostic tool that monitors and records network information?

A. Online monitor
B. Downtime report
C. Help desk report
D. Protocol analyzer

**Answer:** D

**Explanation:**

Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached. Online monitors (choice A) measure telecommunications transmissions and determine whether transmissions were accurate and complete. Downtime reports (choice B) track the availability of telecommunication lines and circuits. Help desk reports (choice C) are prepared by the help desk, which is staffed or supported by IS technical support personnel trained to handle problems occurring during the course of IS operations.

**NEW QUESTION 347**
- (Topic 5)
Which of the following BEST limits the impact of server failures in a distributed environment?

A. Redundant pathways
B. Clustering
C. Dial backup lines
D. Standby power

**Answer:** B

**Explanation:**

Clustering allows two or more servers to work as a unit, so that when one of them fails, the other takes over. Choices A and C are intended to minimize the impact of channel communications failures, but not a server failure. Choice D provides an alternative power source in the event of an energy failure.

**NEW QUESTION 349**
- (Topic 5)
When reviewing a hardware maintenance program, an IS auditor should assess whether:

A. the schedule of all unplanned maintenance is maintaine
B. it is in line with historical trend
C. it has been approved by the IS steering committe
D. the program is validated against vendor specification

**Answer:** D

**Explanation:**

Though maintenance requirements vary based on complexity and performance work loads, a hardware maintenance schedule should be validated against the vendor-provided specifications. For business reasons, an organization may choose a more aggressive maintenance program than the vendor's program. The maintenance program should include maintenance performance history, be it planned, unplanned, executed or exceptional. Unplanned maintenance cannot be scheduled. Hardware maintenance programs do not necessarily need to be in line with historical trends. Maintenance schedules normally are not approved by the steering committee.

**NEW QUESTION 351**
- (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 354**
- (Topic 5)
Which of the following will prevent dangling tuples in a database?

A. Cyclic integrity
B. Domain integrity
C. Relational integrity
D. Referential integrity

**Answer:** D

**Explanation:**

Referential integrity ensures that a foreign key in one table will equal null or the value of a primary in the other table. For every tuple in a table having a referenced/foreign key, there should be a corresponding tuple in another table, i.e., forexistence of all foreign keys in the original tables, if this condition is not satisfied, then it results in a dangling tuple. Cyclical checking is the control technique for the regular checking of accumulated data on a file against authorized sourcedocumentation. There is no cyclical integrity testing. Domain integrity testing ensures that a data item has a legitimate value in the correct range or set. Relational integrity is performed at the record level and is ensured by calculating and verifying specific fields.

**NEW QUESTION 356**
- (Topic 5)
Which of the following controls would provide the GREATEST assurance of database integrity?

A. Audit log procedures
B. Table link/reference checks
C. Query/table access time checks
D. Rollback and rollforward database features

**Answer:** B

**Explanation:**

Performing table link/reference checks serves to detect table linking errors (such as completeness and accuracy of the contents of the database), and thus provides the greatest assurance of database integrity. Audit log procedures enable recording ofall events that have been identified and help in tracing the events. However, they only point to the event and do not ensure completeness or accuracy of the database's contents. Querying/monitoring table access time checks helps designers improve database performance, but not integrity. Rollback and rollforward database features ensure recovery from an abnormal disruption. They assure the integrity of the transaction that was being processed at the time of disruption, but do not provide assurance on the integrity of the contents of 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 363**
- (Topic 5)
An IS auditor finds that, at certain times of the day, the data warehouse query
performance decreases significantly. Which of the following controls would it be relevant for the IS auditor to review?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 367**
- (Topic 5)
Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 368**
- (Topic 5)
Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?

A. Assess the impact of patches prior to installatio
B. Ask the vendors for a new software version with all fixes include
C. install the security patch immediatel
D. Decline to deal with these vendors in the futur

**Answer:** A

**Explanation:**

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

**NEW QUESTION 372**
- (Topic 5)
Change management procedures are established by IS management to:

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 377**
- (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 378**
- (Topic 5)
When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

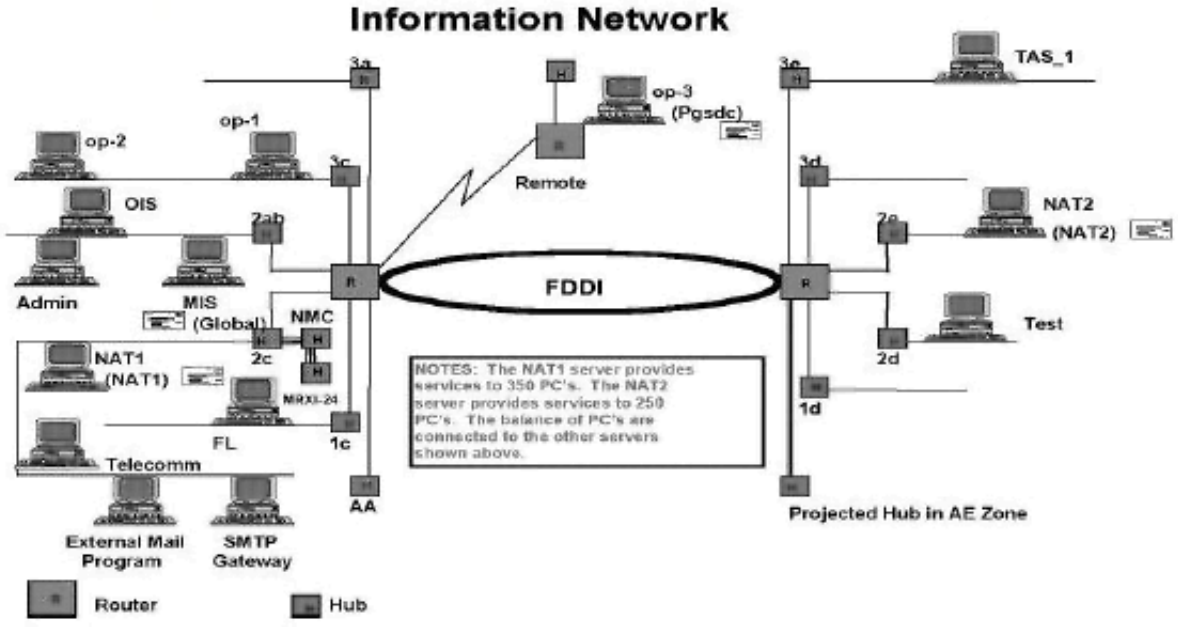
A. allow changes, which will be completed using after-the-fact follow-u
B. allow undocumented changes directly to the production librar
C. do not allow any emergency change
D. allow programmers permanent access to production program

**Answer:** A

**Explanation:**

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

**NEW QUESTION 383**
- (Topic 5)
Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?




A. No firewalls are needed
B. Op-3 location only
C. MIS (Global) and NAT2
D. SMTP Gateway and op-3

**Answer:** D

**Explanation:**

The objective of a firewall is to protect a trusted network from an untrusted network; therefore, locations needing firewall implementations would be at the existence of the external connections. All other answers are incomplete or represent internal connections.

**NEW QUESTION 388**
- (Topic 5)
For locations 3a, 1d and 3d, the diagram indicates hubs with lines that appear to be open and active. Assuming that is true, what control, if any, should be recommended to mitigate this weakness?

A. Intelligent hub
B. Physical security over the hubs
C. Physical security and an intelligent hub
D. No controls are necessary since this is not a weakness

**Answer:** C

**Explanation:**

Open hubs represent a significant control weakness because of the potential to access a network connection easily. An intelligent hub would allow the deactivation of a single port while leaving the remaining ports active. Additionally, physical security would also provide
reasonable protection over hubs with active ports.

**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 393**
- (Topic 5)
The most likely error to occur when implementing a firewall is:

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 397**
- (Topic 5)
Which of the following applet intrusion issues poses the GREATEST risk of disruption to an organization?

A. A program that deposits a virus on a client machine
B. Applets recording keystrokes and, therefore, passwords
C. Downloaded code that reads files on a client's hard drive
D. Applets opening connections from the client machine

**Answer:** D

**Explanation:**

An applet is a program downloaded from a web server to the client, usually through a web browser that provides functionality for database access, interactive web pages and communications with other users. Applets opening connections from the client machine to other machines on the network and damaging those machines, as a denial-of-service attack, pose the greatest threat to an organization and could disrupt business continuity. A program that deposits a virus on a client machine is referred toas a malicious attack (i.e., specifically meant to cause harm to a client machine), but may not necessarily result in a disruption of service. Applets that record keystrokes, and therefore, passwords, and downloaded code that reads files on a client's hard drive relate more to organizational privacy issues, and although significant, are less likely to cause a significant disruption of service.

**NEW QUESTION 399**
- (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 402**
- (Topic 5)
Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 403**
- (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 405**
- (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 409**
- (Topic 6)
To determine who has been given permission to use a particular system resource, an IS auditor should review:

A. activity list
B. access control list
C. logon ID list
D. password list

**Answer:** B

**Explanation:**

Access control lists are the authorization tables that document the users who have been given permission to use a particular system resource and the types of access they have been granted. The other choices would not document who has been given permission to use (access) specific system resources.

**NEW QUESTION 414**
- (Topic 6)
Which of the following is a benefit of using a callback device?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 419**
- (Topic 6)
When performing an audit of access rights, an IS auditor should be suspicious of which of the following if allocated to a computer operator?

A. Read access to data
B. Delete access to transaction data files
C. Logged read/execute access to programs
D. Update access to job control language/script files

**Answer:** B

**Explanation:**

Deletion of transaction data files should be a function of the application support team, not operations staff. Read access to production data is a normal requirement of a computer operator, as is logged access to programs and access to JCL to controljob execution.

**NEW QUESTION 422**
- (Topic 6)
With the help of a security officer, granting access to data is the responsibility of:

A. data owner
B. programmer
C. system analyst
D. librarian

**Answer:** A

**Explanation:**

Data owners are responsible for the use of datA. Written authorization for users to gain access to computerized information should be provided by the data owners. Security administration with the owners' approval sets up access rules stipulating which users or group of users are authorized to access data or files and the level of authorized access (e.g., read or update).

**NEW QUESTION 426**
- (Topic 6)
A hacker could obtain passwords without the use of computer tools or programs through the technique of:

A. social engineerin
B. sniffer
C. back door
D. Trojan horse

**Answer:** A

**Explanation:**

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

**NEW QUESTION 430**
- (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 434**
- (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 437**
- (Topic 6)
Inadequate programming and coding practices introduce the risk of:

A. phishin
B. buffer overflow exploitatio
C. SYN floo
D. brute force attack

**Answer:** B

**Explanation:**

Buffer overflow exploitation may occur when programs do not check the length of the data that are input into a program. An attacker can send data that exceed the length of a buffer and override part of the program with malicious code. The countermeasure is proper programming and good coding practices. Phishing, SYN flood and brute force attacks happen independently of programming and coding practices.

**NEW QUESTION 441**
- (Topic 6)
Which of the following would prevent unauthorized changes to information stored in a server's log?

A. Write-protecting the directory containing the system log
B. Writing a duplicate log to another server
C. Daily printing of the system log
D. Storing the system log in write-once media

**Answer:** D

**Explanation:**

Storing the system log in write-once media ensures the log cannot be modified. Write-protecting the system log does not prevent deletion or modification, since the superuser or users that have special permission can override the write protection. Writing a duplicate log to another server or daily printing of the system log cannot prevent unauthorized changes.

**NEW QUESTION 442**
- (Topic 6)
In an online banking application, which of the following would BEST protect against identity theft?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 444**
- (Topic 6)
Which of the following would MOST effectively enhance the security of a challenge-response based authentication system?

A. Selecting a more robust algorithm to generate challenge strings
B. implementing measures to prevent session hijacking attacks
C. increasing the frequency of associated password changes
D. increasing the length of authentication strings

**Answer:** B

**Explanation:**

Challenge response-based authentication is prone to session hijacking or man-in-the-middle attacks. Security management should be aware of this and engage in risk assessment and control design when they employ this technology. Selecting a more robust algorithm will enhance the security; however, this may not be as important in terms of risk when compared to man-in-the-middle attacks. Choices C and D are good security practices; however, they are not as effective a preventive measure. Frequently changing passwords is a good security practice; however, the exposures lurking in communication pathways may pose a greater risk.

**NEW QUESTION 446**
- (Topic 6)
The responsibility for authorizing access to a business application system belongs to the:

A. data owne
B. security administrato
C. IT security manage
D. requestor's immediate superviso

**Answer:** A

**Explanation:**

When a business application is developed, the best practice is to assign an information or data owner to the application. The Information owner should be responsible for authorizing access to the application itself or to back-end databases for queries. Choices B and C are not correct because the security administrator and manager normally do not have responsibility for authorizing access to business applications. The requestor's immediate supervisor may share the responsibility for approving user access to a business application system; however, the final responsibility should go to the information owner.

**NEW QUESTION 449**
- (Topic 6)
Which of the following intrusion detection systems (IDSs) monitors the general patterns of activity and traffic on a network and creates a database?

A. Signature-based
B. Neural networks-based
C. Statistical-based
D. Host-based

**Answer:** B

**Explanation:**

The neural networks-based IDS monitors the general patterns of activity and traffic on the network and creates a database. This is similar to the statistical model but has the added function of self-learning. Signature-based systems are a type of IDS in which the intrusive patterns identified are stored in the form of signatures. These IDS systems protect against detected intrusion patterns. Statistical-based systems need a comprehensive definition of the known and expected behavior of systems. Host-based systems are not a type of IDS, but a category of IDS, and are configured for a specific environment. They will monitor various internal resources of the operating system to warn of a possible attack.

**NEW QUESTION 453**
.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons and Answers in PDF Format

## CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

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

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