

CISA Dumps

Isaca CISA

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



NEW QUESTION 1

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 2

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 3

- (Topic 1)

Which of the following is a dynamic analysis tool for the purpose of testing software modules?

- A. Blackbox test
- B. Desk checking
- C. Structured walk-through
- D. Design and code

Answer: A

Explanation:

A blackbox test is a dynamic analysis tool for testing software modules. During the testing of software modules a blackbox test works first in a cohesive manner as one single unit/entity, consisting of numerous modules and second, with the user data that flows across software modules. In some cases, this even drives the software behavior.

NEW QUESTION 4

- (Topic 1)

Which of the following is MOST likely to result from a business process reengineering (BPR) project?

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

Answer: A

Explanation:

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

NEW QUESTION 5

- (Topic 1)

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

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

Answer:

B

Explanation:

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

NEW QUESTION 6

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 7

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 8

- (Topic 1)

The use of a GANTT chart can:

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

Answer: A

Explanation:

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

NEW QUESTION 9

- (Topic 1)

Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

- A. A neural network
- B. Database management software
- C. Management information systems
- D. Computer assisted audit techniques

Answer: A

Explanation:

A neural network will monitor and learn patterns, reporting exceptions for investigation.

NEW QUESTION 10

- (Topic 1)

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

- A. Point-of-sale system

- B. Corporate planning
- C. Regulatory reporting
- D. Departmental chargeback

Answer: A

Explanation:

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

NEW QUESTION 10

- (Topic 1)

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

- A. development and implementation of an information security standards manual
- B. performance of a comprehensive security control review by the IS auditor
- C. adoption of a corporate information security policy statement
- D. purchase of security access control software

Answer: C

Explanation:

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

NEW QUESTION 13

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 16

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 19

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 24

- (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 value
- B. Greater value
- C. Lesser value
- D. Prior audit reports are not relevant

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 25

- (Topic 1)

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

- A. Controls testing starts earlier
- B. Auditing resources are allocated to the areas of highest concern
- C. Auditing risk is reduced
- D. Controls testing is more thorough

Answer: B

Explanation:

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

NEW QUESTION 29

- (Topic 1)

The use of statistical sampling procedures helps minimize:

- A. Detection risk
- B. Business risk
- C. Controls risk
- D. Compliance risk

Answer: A

Explanation:

The use of statistical sampling procedures helps minimize detection risk.

NEW QUESTION 32

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 33

- (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 35

- (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 36

- (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 40

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 41

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 44

- (Topic 1)

Which of the following do digital signatures provide?

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

Answer: A

Explanation:

The primary purpose of digital signatures is to provide authentication and integrity of data.

NEW QUESTION 48

- (Topic 1)

Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

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

Answer: A

Explanation:

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

NEW QUESTION 52

- (Topic 1)

What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources? Choose the BEST answer.

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

Answer: C

Explanation:

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

NEW QUESTION 54

- (Topic 1)

What is the key distinction between encryption and hashing algorithms?

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

Answer: B

Explanation:

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

NEW QUESTION 59

- (Topic 1)

What type of BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness?

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

Answer: B

Explanation:

Of the three major types of BCP tests (paper, walk-through, and preparedness), only the preparedness test uses actual resources to simulate a system crash and validate the plan's effectiveness.

NEW QUESTION 61

- (Topic 1)

Which of the following typically focuses on making alternative processes and resources available for transaction processing?

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

Answer: D

Explanation:

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

NEW QUESTION 66

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 70

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 71

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 76

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 78

- (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 80

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 82

- (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 85

- (Topic 1)

What can be used to help identify and investigate unauthorized transactions? Choose the BEST answer.

- A. Postmortem review
- B. Reasonableness checks
- C. Data-mining techniques
- D. Expert systems

Answer: C

Explanation:

Data-mining techniques can be used to help identify and investigate unauthorized transactions.

NEW QUESTION 90

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 93

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 97

- (Topic 1)

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

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

Answer: A

Explanation:

A completeness check is an edit check to determine whether a field contains valid data.

NEW QUESTION 101

- (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 106

- (Topic 1)

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

- A. Text search forensic utility software

- B. Generalized audit software
- C. Productivity audit software
- D. Manual review

Answer: B

Explanation:

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

NEW QUESTION 108

- (Topic 1)

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

- A. True
- B. False

Answer: B

Explanation:

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

NEW QUESTION 110

- (Topic 1)

Who is responsible for implementing cost-effective controls in an automated system?

- A. Security policy administrators
- B. Business unit management
- C. Senior management
- D. Board of directors

Answer: B

Explanation:

Business unit management is responsible for implementing cost-effective controls in an automated system.

NEW QUESTION 113

- (Topic 1)

Why does an IS auditor review an organization chart?

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

Answer: C

Explanation:

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

NEW QUESTION 114

- (Topic 1)

What can be implemented to provide the highest level of protection from external attack?

- A. Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
- B. Configuring the firewall as a screened host behind a router
- C. Configuring the firewall as the protecting bastion host
- D. Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Answer: A

Explanation:

Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host provides a higher level of protection from external attack than all other answers.

NEW QUESTION 117

- (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 121

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 126

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 130

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 134

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 139

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 144

- (Topic 1)

What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

- A. An organizational certificate
- B. A user certificate

- C. A website certificate
- D. Authenticode

Answer: C

Explanation:

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

NEW QUESTION 145

- (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 147

- (Topic 1)

Which of the following is of greatest concern when performing an IS audit?

- A. Users' ability to directly modify the database
- B. Users' ability to submit queries to the database
- C. Users' ability to indirectly modify the database
- D. Users' ability to directly view the database

Answer: A

Explanation:

A major IS audit concern is users' ability to directly modify the database.

NEW QUESTION 151

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 152

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 157

- (Topic 1)

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

- A. True
- B. False

Answer: B

Explanation:

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

NEW QUESTION 160

- (Topic 1)

Which of the following is the dominating objective of BCP and DRP?

- A. To protect human life
- B. To mitigate the risk and impact of a business interruption
- C. To eliminate the risk and impact of a business interruption
- D. To transfer the risk and impact of a business interruption

Answer: A

Explanation:

Although the primary business objective of BCP and DRP is to mitigate the risk and impact of a business interruption, the dominating objective remains the protection of human life.

NEW QUESTION 165

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 169

- (Topic 1)

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

- A. Develop test plan
- B. Baseline procedures to prevent scope creep
- C. Define the need that requires resolution, and map to the major requirements of the solution
- D. Program and test the new system
- E. The tests verify and validate what has been developed

Answer: B

Explanation:

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

NEW QUESTION 172

- (Topic 1)

When should application controls be considered within the system-development process?

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

Answer: D

Explanation:

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

NEW QUESTION 175

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 178

- (Topic 1)

Which of the following uses a prototype that can be updated continually to meet changing user or business requirements?

- A. PERT
- B. Rapid application development (RAD)
- C. Function point analysis (FPA)
- D. GANTT

Answer: B

Explanation:

Rapid application development (RAD) uses a prototype that can be updated continually to meet changing user or business requirements.

NEW QUESTION 183

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 184

- (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 187

- (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 190

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 194

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 198

- (Topic 1)

An IS auditor is using a statistical sample to inventory the tape library. What type of test would this be considered?

- A. Substantive
- B. Compliance
- C. Integrated
- D. Continuous audit

Answer: A

Explanation:

Using a statistical sample to inventory the tape library is an example of a substantive test.

NEW QUESTION 203

- (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 204

- (Topic 2)

Overall business risk for a particular threat can be expressed as:

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

Answer: A

Explanation:

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

NEW QUESTION 205

- (Topic 2)

Which of the following sampling methods is MOST useful when testing for compliance?

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

Answer: A

Explanation:

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

NEW QUESTION 208

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 209

- (Topic 2)

An IS auditor evaluating logical access controls should FIRST:

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

Answer: D

Explanation:

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

NEW QUESTION 214

- (Topic 2)

The PRIMARY purpose of an IT forensic audit is:

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

Answer: B

Explanation:

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

NEW QUESTION 219

- (Topic 2)

In an IS audit of several critical servers, the IS auditor wants to analyze audit trails to discover potential anomalies in user or system behavior. Which of the following tools are MOST suitable for performing that task?

- A. CASE tools
- B. Embedded data collection tools
- C. Heuristic scanning tools
- D. Trend/variance detection tools

Answer: D

Explanation:

Trend/variance detection tools look for anomalies in user or system behavior, for example, determining whether the numbers for prenumbered documents are sequential or increasing. CASE tools are used to assist software development. Embedded (audit) data collection software is used for sampling and to provide production statistics. Heuristic scanning tools can be used to scan for viruses to indicate possible infected code.

NEW QUESTION 220

CORRECT TEXT - (Topic 2)

The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

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

Answer: B

NEW QUESTION 222

- (Topic 2)

In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

- A. identify and assess the risk assessment process used by management
- B. identify information assets and the underlying system
- C. disclose the threats and impacts to management
- D. identify and evaluate the existing control

Answer: D

Explanation:

It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

NEW QUESTION 227

- (Topic 2)

An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

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

Answer: A

Explanation:

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

NEW QUESTION 229

- (Topic 2)

While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?

- A. Observe the response mechanism
- B. Clear the virus from the network
- C. Inform appropriate personnel immediately
- D. Ensure deletion of the virus

Answer: C

Explanation:

The first thing an IS auditor should do after detecting the virus is to alert the organization to its presence, then wait for their response. Choice A should be taken after choice C. This will enable an IS auditor to examine the actual workability and effectiveness of the response system. An IS auditor should not make changes to the system being audited, and ensuring the deletion of the virus is a management responsibility.

NEW QUESTION 232

- (Topic 2)

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

- A. professional independence
- B. organizational independence
- C. technical competence
- D. professional competence

Answer: A

Explanation:

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

NEW QUESTION 237

- (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 personnel
- B. detect a source program change made between acquiring a copy of the source and the comparison run
- C. confirm that the control copy is the current version of the production program
- D. ensure that all changes made in the current source copy are detected

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 240

- (Topic 2)

The final decision to include a material finding in an audit report should be made by the:

- A. audit committee
- B. auditee's manager
- C. IS auditor
- D. CEO of the organization

Answer: C

Explanation:

The IS auditor should make the final decision about what to include or exclude from the audit report. The other choices would limit the independence of the auditor.

NEW QUESTION 243

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 245

- (Topic 3)

Involvement of senior management is MOST important in the development of:

- A. strategic plan
- B. IS policies
- C. IS procedure
- D. standards and guideline

Answer: A

Explanation:

Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives. IS policies, procedures, standards and guidelines are all structured to support the overall strategic plan.

NEW QUESTION 247

- (Topic 3)

Which of the following IT governance best practices improves strategic alignment?

- A. Supplier and partner risks are managed
- B. A knowledge base on customers, products, markets and processes is in place
- C. A structure is provided that facilitates the creation and sharing of business information
- D. Top management mediate between the imperatives of business and technology

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 and processes 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 252

- (Topic 3)

Which of the following is the MOST important element for the successful implementation of IT governance?

- A. Implementing an IT scorecard

- B. Identifying organizational strategies
- C. Performing a risk assessment
- D. Creating a formal security policy

Answer: B

Explanation:

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

NEW QUESTION 254

- (Topic 3)

The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

- A. IT budget
- B. existing IT environment
- C. business plan
- D. investment plan

Answer: C

Explanation:

One of the most important reasons for which projects get funded is how well a project meets an organization's strategic objectives. Portfolio management takes a holistic view of a company's overall IT strategy. IT strategy should be aligned with the business strategy and, hence, reviewing the business plan should be the major consideration. Choices A, B and D are important but secondary to the importance of reviewing the business plan.

NEW QUESTION 259

- (Topic 3)

The ultimate purpose of IT governance is to:

- A. encourage optimal use of IT
- B. reduce IT cost
- C. decentralize IT resources across the organization
- D. centralize control of IT

Answer: A

Explanation:

IT governance is intended to specify the combination of decision rights and accountability that is best for the enterprise. It is different for every enterprise. Reducing IT costs may not be the best IT governance outcome for an enterprise. Decentralizing IT resources across the organization is not always desired, although it may be desired in a decentralized environment. Centralizing control of IT is not always desired. An example of where it might be desired is an enterprise desiring a single point of customer contact.

NEW QUESTION 261

- (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 264

- (Topic 3)

Responsibility for the governance of IT should rest with the:

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

Answer: D

Explanation:

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

NEW QUESTION 267

- (Topic 3)

To support an organization's goals, an IS department should have:

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

Answer: B

Explanation:

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

NEW QUESTION 270

- (Topic 3)

An IS auditor reviewing an organization's IT strategic plan should FIRST review:

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

Answer: B

Explanation:

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

NEW QUESTION 275

- (Topic 3)

In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

- A. Optimized
- B. Managed
- C. Defined
- D. Repeatable

Answer: B

Explanation:

Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable.'

NEW QUESTION 277

- (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 281

- (Topic 3)

The development of an IS security policy is ultimately the responsibility of the:

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

Answer: D

Explanation:

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

NEW QUESTION 286

- (Topic 3)

Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

- A. Response
- B. Correction
- C. Detection
- D. Monitoring

Answer: A

Explanation:

A sound IS security policy will most likely outline a response program to handle suspected intrusions. Correction, detection and monitoring programs are all aspects of information security, but will not likely be included in an IS security policy statement.

NEW QUESTION 291

- (Topic 3)

The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

- A. Utilization of an intrusion detection system to report incidents
- B. Mandating the use of passwords to access all software
- C. Installing an efficient user log system to track the actions of each user
- D. Training provided on a regular basis to all current and new employees

Answer: D

Explanation:

Utilizing an intrusion detection system to report on incidents that occur is an implementation of a security program and is not effective in establishing a security awareness program. Choices B and C do not address awareness. Training is the only choice that is directed at security awareness.

NEW QUESTION 295

- (Topic 3)

In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

- A. implementatio
- B. complianc
- C. documentatio
- D. sufficienc

Answer: D

Explanation:

An IS auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of controls. Documentation, implementation and compliance are further steps.

NEW QUESTION 298

- (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 301

- (Topic 3)

Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?

- A. Define a balanced scorecard (BSC) for measuring performance
- B. Consider user satisfaction in the key performance indicators (KPIs)
- C. Select projects according to business benefits and risks
- D. Modify the yearly process of defining the project portfolio

Answer: C

Explanation:

Prioritization of projects on the basis of their expected benefit(s) to business, and the related risks, is the best measure for achieving alignment of the project portfolio to an organization's strategic priorities. Modifying the yearly process of the projects portfolio definition might improve the situation, but only if the portfolio definition process is currently not tied to the definition of corporate strategies; however, this is unlikely since the difficulties are in maintaining the alignment, and not in setting it up initially. Measures such as balanced scorecard (BSC) and key performance indicators (KPIs) are helpful, but they do not guarantee that the projects are aligned with business strategy.

NEW QUESTION 306

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 308

- (Topic 3)

In the context of effective information security governance, the primary objective of value delivery is to:

- A. optimize security investments in support of business objective
- B. implement a standard set of security practice
- C. institute a standards-based solution
- D. implement a continuous improvement culture

Answer: A

Explanation:

In the context of effective information security governance, value delivery is implemented to ensure optimization of security investments in support of business objectives. The tools and techniques for implementing value delivery include implementation of a standard set of security practices, institutionalization and commoditization of standards-based solutions, and implementation of a continuous improvement culture considering security as a process, not an event.

NEW QUESTION 309

- (Topic 3)

After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

- A. Project management and progress reporting is combined in a project management office which is driven by external consultant
- B. The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach
- C. The resources of each of the organizations are inefficiently allocated while they are being familiarized with the other company's legacy system
- D. The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training need

Answer: B

Explanation:

The efforts should be consolidated to ensure alignment with the overall strategy of the postmerger organization. If resource allocation is not centralized, the separate projects are at risk of overestimating the availability of key knowledge resources for the in-house developed legacy applications. In postmerger integration programs, it is common to form project management offices to ensure standardized and comparable information levels in the planning and reporting structures, and to centralized dependencies of project deliverables or resources. The experience of external consultants can be valuable since project management practices do not require in-depth knowledge of the legacy systems. This can free up resources for functional tasks. It is a good idea to first get familiar with the old systems, to understand what needs to be done in a migration and to evaluate the implications of technical decisions. In most cases, mergers result in application changes and thus in training needs as organizations and processes change to leverage the intended synergy effects of the merger.

NEW QUESTION 314

- (Topic 3)

Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

- A. Ensuring that invoices are paid to the provider
- B. Participating in systems design with the provider

- C. Renegotiating the provider's fees
- D. Monitoring the outsourcing provider's performance

Answer: D

Explanation:

In an outsourcing environment, the company is dependent on the performance of the service provider. Therefore, it is critical the outsourcing provider's performance be monitored to ensure that services are delivered to the company as required. Payment of invoices is a finance function, which would be completed per contractual requirements. Participating in systems design is a byproduct of monitoring the outsourcing provider's performance, while renegotiating fees is usually a one-time activity.

NEW QUESTION 316

- (Topic 3)

An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine FIRST?

- A. That an audit clause is present in all contracts
- B. That the SLA of each contract is substantiated by appropriate KPIs
- C. That the contractual warranties of the providers support the business needs of the organization
- D. That at contract termination, support is guaranteed by each outsourcer for new outsourcers

Answer: C

Explanation:

The complexity of IT structures matched by the complexity and interplay of responsibilities and warranties may affect or void the effectiveness of those warranties and the reasonable certainty that the business needs will be met. All other choices are important, but not as potentially dangerous as the interplay of the diverse and critical areas of the contractual responsibilities of the outsourcers.

NEW QUESTION 320

- (Topic 3)

While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern should be that the:

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

Answer: A

Explanation:

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

NEW QUESTION 322

- (Topic 3)

Which of the following is a mechanism for mitigating risks?

- A. Security and control practices
- B. Property and liability insurance
- C. Audit and certification
- D. Contracts and service level agreements (SLAs)

Answer: A

Explanation:

Risks are mitigated by implementing appropriate security and control practices. Insurance is a mechanism for transferring risk. Audit and certification are mechanisms of risk assurance, while contracts and SLAs are mechanisms of risk allocation.

NEW QUESTION 324

- (Topic 3)

To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

- A. avoidance
- B. transference
- C. mitigation
- D. acceptance

Answer: C

Explanation:

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

NEW QUESTION 329

- (Topic 3)

An IS auditor who is reviewing incident reports discovers that, in one instance, an important document left on an employee's desk was removed and put in the garbage by the outsourced cleaning staff. Which of the following should the IS auditor recommend to management?

- A. Stricter controls should be implemented by both the organization and the cleaning agency
- B. No action is required since such incidents have not occurred in the past
- C. A clear desk policy should be implemented and strictly enforced in the organization
- D. A sound backup policy for all important office documents should be implemented

Answer: A

Explanation:

An employee leaving an important document on a desk and the cleaning staff removing it may result in a serious impact on the business. Therefore, the IS auditor should recommend that strict controls be implemented by both the organization and the outsourced cleaning agency. That such incidents have not occurred in the past does not reduce the seriousness of their impact. Implementing and monitoring a clear desk policy addresses only one part of the issue. Appropriate confidentiality agreements with the cleaning agency, along with ensuring that the cleaning staff has been educated on the dos and don'ts of the cleaning process, are also controls that should be implemented. The risk here is not a loss of data, but leakage of data to unauthorized sources. A backup policy does not address the issue of unauthorized leakage of information.

NEW QUESTION 332

- (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 337

- (Topic 4)

Documentation of a business case used in an IT development project should be retained until:

- A. the end of the system's life cycle
- B. the project is approved
- C. user acceptance of the system
- D. the system is in production

Answer: A

Explanation:

A business case can and should be used throughout the life cycle of the product. It serves as an anchor for new (management) personnel, helps to maintain focus and provides valuable information on estimates vs. actuals. Questions like, 'why do we do that,' 'what was the original intent' and 'how did we perform against the plan' can be answered, and lessons for developing future business cases can be learned. During the development phase of a project one should always validate the business case, as it is a good management instrument. After finishing a project and entering production, the business case and all the completed research are valuable sources of information that should be kept for further reference.

NEW QUESTION 341

- (Topic 4)

Change control for business application systems being developed using prototyping could be complicated by the:

- A. iterative nature of prototyping
- B. rapid pace of modifications in requirements and design
- C. emphasis on reports and screen
- D. lack of integrated tool

Answer: B

Explanation:

Changes in requirements and design happen so quickly that they are seldom documented or approved. Choices A, C and D are characteristics of prototyping, but they do not have an adverse effect on change control.

NEW QUESTION 342

- (Topic 4)

When planning to add personnel to tasks imposing time constraints on the duration of a project, which of the following should be revalidated FIRST?

- A. The project budget
- B. The critical path for the project
- C. The length of the remaining tasks
- D. The personnel assigned to other tasks

Answer: B

Explanation:

Since adding resources may change the route of the critical path, the critical path must be reevaluated to ensure that additional resources will in fact shorten the project duration. Given that there may be slack time available on some of the other tasks not on the critical path, factors such as the project budget, the length of other tasks and the personnel assigned to them may or may not be affected.

NEW QUESTION 344

- (Topic 4)

When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

- A. whose sum of activity time is the shortest
- B. that have zero slack time
- C. that give the longest possible completion time
- D. whose sum of slack time is the shortest

Answer: B

Explanation:

A critical path's activity time is longer than that for any other path through the network. This path is important because if everything goes as scheduled, its length gives the shortest possible completion time for the overall project. Activities on the critical path become candidates for crashing, i.e., for reduction in their time by payment of a premium for early completion. Activities on the critical path have zero slack time and conversely, activities with zero slack time are on a critical path. By successively relaxing activities on a critical path, a curve showing total project costs vs. time can be obtained.

NEW QUESTION 347

- (Topic 4)

At the completion of a system development project, a postproject review should include which of the following?

- A. Assessing risks that may lead to downtime after the production release
- B. Identifying lessons learned that may be applicable to future projects
- C. Verifying the controls in the delivered system are working
- D. Ensuring that test data are deleted

Answer: B

Explanation:

A project team has something to learn from each and every project. As risk assessment is a key issue for project management, it is important for the organization to accumulate lessons learned and integrate them into future projects. An assessment of potential downtime should be made with the operations group and other specialists before implementing a system. Verifying that controls are working should be covered during the acceptance test phase and possibly, again, in the postimplementation review. Test data should be retained for future regression testing.

NEW QUESTION 348

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 350

- (Topic 4)

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

- A. Project sponsor

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

Answer: C

Explanation:

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

NEW QUESTION 353

- (Topic 4)

A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

- A. IS auditor
- B. Database administrator
- C. Project manager
- D. Data owner

Answer: D

Explanation:

During the data conversion stage of a project, the data owner is primarily responsible for reviewing and signing-off that the data are migrated completely, accurately and are valid. An IS auditor is not responsible for reviewing and signing-off on the accuracy of the converted data. However, an IS auditor should ensure that there is a review and sign-off by the data owner during the data conversion stage of the project. A database administrator's primary responsibility is to maintain the integrity of the database and make the database available to users. A database administrator is not responsible for reviewing migrated data. A project manager provides day-to-day management and leadership of the project, but is not responsible for the accuracy and integrity of the data.

NEW QUESTION 355

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 356

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 361

- (Topic 4)

The editing/validation of data entered at a remote site would be performed MOST effectively at the:

- A. central processing site after running the application system
- B. central processing site during the running of the application system
- C. remote processing site after transmission of the data to the central processing site
- D. remote processing site prior to transmission of the data to the central processing site

Answer: D

Explanation:

It is important that the data entered from a remote site is edited and validated prior to transmission to the central processing site.

NEW QUESTION 363

- (Topic 4)

What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

- A. Test data/deck
- B. Base-case system evaluation
- C. Integrated test facility (ITF)
- D. Parallel simulation

Answer: B

Explanation:

A base-case system evaluation uses test data sets developed as part of comprehensive testing programs, it is used to verify correct systems operations before acceptance, as well as periodic validation. Test data/deck simulates transactions through real programs. An ITF creates fictitious files in the database with test transactions processed simultaneously with live input. Parallel simulation is the production of data processed using computer programs that simulate application program logic.

NEW QUESTION 366

- (Topic 4)

Which of the following data validation edits is effective in detecting transposition and transcription errors?

- A. Range check
- B. Check digit
- C. Validity check
- D. Duplicate check

Answer: B

Explanation:

A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered, e.g., an incorrect, but valid, value substituted for the original. This control is effective in detecting transposition and transcription errors. A range check is checking data that matches a predetermined range of values. A validity check is programmed checking of the data validity in accordance with predetermined criteria. In a duplicate check, new or fresh transactions are matched to those previously entered to ensure that they are not already in the system.

NEW QUESTION 371

- (Topic 4)

Which of the following is the GREATEST risk to the effectiveness of application system controls?

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

Answer: C

Explanation:

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

NEW QUESTION 373

- (Topic 4)

The MAIN purpose of a transaction audit trail is to:

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

Answer: B

Explanation:

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

NEW QUESTION 378

- (Topic 4)

A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

- A. Establishing an inter-networked system of client servers with suppliers for increased efficiencies
- B. Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing
- C. Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format
- D. Reengineering the existing processing and redesigning the existing system

Answer: C

Explanation:

EDI is the best answer. Properly implemented (e.g., agreements with trading partners transaction standards, controls over network security mechanisms in conjunction with application controls), EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

NEW QUESTION 383

- (Topic 4)

Failure in which of the following testing stages would have the GREATEST impact on the implementation of new application software?

- A. System testing
- B. Acceptance testing
- C. Integration testing
- D. Unit testing

Answer: B

Explanation:

Acceptance testing is the final stage before the software is installed and is available for use. The greatest impact would occur if the software fails at the acceptance testing level, as this could result in delays and cost overruns. System testing is undertaken by the developer team to determine if the software meets user requirements per specifications. Integration testing examines the units/modules as one integrated system and unit testing examines the individual units or components of the software. System, integration and unit testing are all performed by the developers at various stages of development; the impact of failure is comparatively less for each than failure at the acceptance testing stage.

NEW QUESTION 386

- (Topic 4)

An organization has an integrated development environment (IDE) on which the program libraries reside on the server, but modification/development and testing are done from PC workstations. Which of the following would be a strength of an IDE?

- A. Controls the proliferation of multiple versions of programs
- B. Expands the programming resources and aids available
- C. Increases program and processing integrity
- D. Prevents valid changes from being overwritten by other changes

Answer: B

Explanation:

A strength of an IDE is that it expands the programming resources and aids available. The other choices are IDE weaknesses.

NEW QUESTION 388

- (Topic 4)

Ideally, stress testing should be carried out in a:

- A. test environment using test data
- B. production environment using live workload
- C. test environment using live workload
- D. production environment using test data

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 B and D), and if only test data is used, there is no certainty that the system was stress tested adequately.

NEW QUESTION 389

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 390

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 391

- (Topic 4)

Which testing approach is MOST appropriate to ensure that internal application interface errors are identified as soon as possible?

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

Answer: C

Explanation:

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

NEW QUESTION 394

- (Topic 4)

During the system testing phase of an application development project the IS auditor should review the:

- A. conceptual design specification
- B. vendor contract
- C. error report
- D. program change request

Answer: C

Explanation:

Testing is crucial in determining that user requirements have been validated. The IS auditor should be involved in this phase and review error reports for their precision in recognizing erroneous data and review the procedures for resolving errors. A conceptual design specification is a document prepared during the requirements definition phase. A vendor contract is prepared during a software acquisition process. Program change requests would normally be reviewed as a part of the postimplementation phase.

NEW QUESTION 396

- (Topic 4)

The specific advantage of white box testing is that it:

- A. verifies a program can operate successfully with other parts of the system
- B. ensures a program's functional operating effectiveness without regard to the internal program structure
- C. determines procedural accuracy or conditions of a program's specific logic path
- D. examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system

Answer: C

Explanation:

White box testing assesses the effectiveness of software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's logic paths. Verifying the program can operate successfully with other parts of the system is sociability testing. Testing the program's functionality without knowledge of internal structures is black box testing. Controlled testing of programs in a semi-debugged environment, either heavily controlled step-by-step or via monitoring in virtual machines, is sand box testing.

NEW QUESTION 399

- (Topic 4)

Following best practices, formal plans for implementation of new information systems are developed during the:

- A. development phas
- B. design phas
- C. testing phas
- D. deployment phas

Answer: B

Explanation:

Planning for implementation should begin well in advance of the actual implementation date. A formal implementation plan should be constructed in the design phase and revised as the development progresses.

NEW QUESTION 401

- (Topic 4)

An IS auditor is reviewing a project that is using an Agile software development approach. Which of the following should the IS auditor expect to find?

- A. Use of a process-based maturity model such as the capability maturity model (CMM)
- B. Regular monitoring of task-level progress against schedule
- C. Extensive use of software development tools to maximize team productivity
- D. Postiteration reviews that identify lessons learned for future use in the project

Answer: D

Explanation:

A key tenet of the Agile approach to software project management is team learning and the use of team learning to refine project management and software development processes as the project progresses. One of the best ways to achieve this is that, at the end of each iteration, the team considers and documents what worked well and what could have worked better, and identifies improvements to be implemented in subsequent iterations. CMM and Agile really sit at opposite poles. CMM places heavy emphasis on predefined formal processes and formal project management and software development deliverables. Agile projects, by contrast, rely on refinement of process as dictated by the particular needs of the project and team dynamics. Additionally, less importance is placed on formal paper-based deliverables, with the preference being effective informal communication within the team and with key outside contributors. Agile projects produce releasable software in short iterations, typically ranging from 4 to 8 weeks. This, in itself, instills considerable performance discipline within the team. This, combined with short daily meetings to agree on what the team is doing and the identification of any impediments, renders task-level tracking against a schedule redundant. Agile projects do make use of suitable development tools; however, tools are not seen as the primary means of achieving productivity. Team harmony, effective communications and collective ability to solve challenges are of

NEW QUESTION 404

- (Topic 4)

At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

- A. report the error as a finding and leave further exploration to the auditee's discretion
- B. attempt to resolve the error
- C. recommend that problem resolution be escalated
- D. ignore the error, as it is not possible to get objective evidence for the software error

Answer: C

Explanation:

When an IS auditor observes such conditions, it is best to fully apprise the auditee and suggest that further problem resolutions be attempted. Recording it as a minor error and leaving it to the auditee's discretion would be inappropriate, and neglecting the error would indicate that the auditor has not taken steps to further probe the issue to its logical end.

NEW QUESTION 406

- (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 407

- (Topic 4)

An organization is migrating from a legacy system to an enterprise resource planning (ERP) system. While reviewing the data migration activity, the MOST important concern for the IS auditor is to determine that there is a:

- A. correlation of semantic characteristics of the data migrated between the two systems

- B. correlation of arithmetic characteristics of the data migrated between the two system
- C. correlation of functional characteristics of the processes between the two system
- D. relative efficiency of the processes between the two system

Answer: A

Explanation:

Due to the fact that the two systems could have a different data representation, including the database schema, the IS auditor's main concern should be to verify that the interpretation of the data is the same in the new as it was in the old system. Arithmetic characteristics represent aspects of data structure and internal definition in the database, and therefore are less important than the semantic characteristics. A review of the correlation of the functional characteristics or a review of the relative efficiencies of the processes between the two systems is not relevant to a data migration review.

NEW QUESTION 409

- (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 410

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 414

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 419

- (Topic 4)

A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:

- A. payroll reports should be compared to input form
- B. gross payroll should be recalculated manuall
- C. checks (cheques) should be compared to input form
- D. checks (cheques) should be reconciled with output report

Answer: A

Explanation:

The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports. Hence, comparing payroll reports with input forms is the best mechanism of verifying data accuracy. Recalculating gross payroll manually would only verify whether the processing is correct and not the data accuracy of inputs. Comparing checks (cheques) to input forms is not feasible as checks (cheques) have the processed information and input forms have the input data. Reconciling checks (cheques) with output reports only confirms that checks (cheques) have been issued as per output reports.

NEW QUESTION 423

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 425

- (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 into quality (accurate) data.

NEW QUESTION 429

- (Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 431

- (Topic 4)

An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

- A. reverse engineering
- B. prototyping
- C. software reuse
- D. reengineering

Answer: D

Explanation:

Old (legacy) systems that have been corrected, adapted and enhanced extensively require reengineering to remain maintainable. Reengineering is a rebuilding activity to incorporate new technologies into existing systems. Using program language statements, reverse engineering involves reversing a program's machine code into the source code in which it was written to identify malicious content in a program, such as a virus, or to adapt a program written for use with one processor for use with a differently designed processor. Prototyping is the development of a system through controlled trial and error. Software reuse is the process of planning, analyzing and using previously developed software components. The reusable components are integrated into the current software product systematically.

NEW QUESTION 436

- (Topic 5)

IT best practices for the availability and continuity of IT services should:

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

Answer: C

Explanation:

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

NEW QUESTION 439

- (Topic 5)

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

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

Answer: C

Explanation:

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

NEW QUESTION 442

- (Topic 5)

Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

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

Answer: B

Explanation:

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

NEW QUESTION 446

- (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 system access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

NEW QUESTION 449

- (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 authorization
- C. Unauthorized report copies can be printed
- D. Output can be lost in the event of system failure

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 450

- (Topic 5)

Applying a retention date on a file will ensure that:

- A. data cannot be read until the date is set
- B. data will not be deleted before that date
- C. backup copies are not retained after that date
- D. datasets having the same name are differentiated

Answer: B

Explanation:

A retention date will ensure that a file cannot be overwritten before that date has passed. The retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and therefore may be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

NEW QUESTION 452

- (Topic 5)

IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

- A. The outsourcing contract does not cover disaster recovery for the outsourced IT operation
- B. The service provider does not have incident handling procedure
- C. Recently a corrupted database could not be recovered because of library management problem
- D. incident logs are not being reviewed

Answer: A

Explanation:

The lack of a disaster recovery provision presents a major business risk. Incorporating such a provision into the contract will provide the outsourcing organization leverage over the service provider. Choices B, C and D are problems that should be addressed by the service provider, but are not as important as contract requirements for disaster recovery.

NEW QUESTION 453

- (Topic 5)

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

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

Answer: C

Explanation:

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

NEW QUESTION 455

- (Topic 5)

The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

- A. loss of confidentiality
- B. increased redundancy
- C. unauthorized access
- D. application malfunction

Answer: B

Explanation:

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

NEW QUESTION 459

- (Topic 5)

The BEST way to minimize the risk of communication failures in an e-commerce environment would be to use:

- A. compression software to minimize transmission duration
- B. functional or message acknowledgment
- C. a packet-filtering firewall to reroute message
- D. leased asynchronous transfer mode line

Answer: D**Explanation:**

Leased asynchronous transfer mode lines are a way to avoid using public and shared infrastructures from the carrier or Internet service provider that have a greater number of communication failures. Choice A, compression software, is a valid way to reduce the problem, but is not as good as leased asynchronous transfer mode lines. Choice B is a control based on higher protocol layers and helps if communication lines are introducing noise, but not if a link is down. Choice C, a packet-filtering firewall, does not reroute messages.

NEW QUESTION 460

- (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 465

- (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 468

- (Topic 5)

Which of the following is the BEST type of program for an organization to implement to aggregate, correlate and store different log and event files, and then produce weekly and monthly reports for IS auditors?

- A. A security information event management (SIEM) product
- B. An open-source correlation engine
- C. A log management tool
- D. An extract, transform, load (ETL) system

Answer: C**Explanation:**

A log management tool is a product designed to aggregate events from many log files (with distinct formats and from different sources), store them and typically correlate them offline to produce many reports (e.g., exception reports showing different statistics including anomalies and suspicious activities), and to answer time-based queries (e.g., how many users have entered the system between 2 a.m. and 4 a.m. over the past three weeks?). A SIEM product has some similar features. It correlates events from log files, but does it online and normally is not oriented to storing many weeks of historical information and producing audit reports. A correlation engine is part of a SIEM product. It is oriented to making an online correlation of events. An extract, transform, load (ETL) is part of a business intelligence system, dedicated to extracting operational or production data, transforming that data and loading them to a central repository (data warehouse or data mart); an ETL does not correlate data or produce reports, and normally it does not have extractors to read log file formats.

NEW QUESTION 470

- (Topic 5)

Which of the following would BEST maintain the integrity of a firewall log?

- A. Granting access to log information only to administrators
- B. Capturing log events in the operating system layer

- C. Writing dual logs onto separate storage media
- D. Sending log information to a dedicated third-party log server

Answer: D

Explanation:

Establishing a dedicated third-party log server and logging events in it is the best procedure for maintaining the integrity of a firewall log. When access control to the log server is adequately maintained, the risk of unauthorized log modification will be mitigated, therefore improving the integrity of log information. To enforce segregation of duties, administrators should not have access to log files. This primarily contributes to the assurance of confidentiality rather than integrity. There are many ways to capture log information: through the application layer, network layer, operating systems layer, etc.; however, there is no log integrity advantage in capturing events in the operating systems layer. If it is a highly mission-critical information system, it may be nice to run the system with a dual log mode. Having logs in two different storage devices will primarily contribute to the assurance of the availability of log information, rather than to maintaining its integrity.

NEW QUESTION 474

- (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., foreexistence 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 478

- (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 of all 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 480

- (Topic 5)

During maintenance of a relational database, several values of the foreign key in a transaction table of a relational database have been corrupted. The consequence is that:

- A. the detail of involved transactions may no longer be associated with master data, causing errors when these transactions are processed
- B. there is no way of reconstructing the lost information, except by deleting the dangling tuples and reentering the transaction
- C. the database will immediately stop execution and lose more information
- D. the database will no longer accept input data

Answer: A

Explanation:

When the external key of a transaction is corrupted or lost, the application system will normally be incapable of directly attaching the master data to the transaction data. This will normally cause the system to undertake a sequential search and slow down the processing. If the concerned files are big, this slowdown will be unacceptable. Choice B is incorrect, since a system can recover the corrupted external key by reindexing the table. Choices C and D would not result from a corrupted foreign key.

NEW QUESTION 481

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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