



Isaca

Exam Questions CISA

Isaca CISA

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

- (Topic 1)

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 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 3

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 4

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

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 5

- (Topic 1)

Which of the following network configuration options contains a direct link between any two host machines?

- A. Bus
- B. Ring
- C. Star

D. Completely connected (mesh)

Answer: D

Explanation:

A completely connected mesh configuration creates a direct link between any two host machines.

NEW QUESTION 6

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 7

- (Topic 1)

Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

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

Answer: D

Explanation:

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

NEW QUESTION 8

- (Topic 1)

A hardware control that helps to detect errors when data are communicated from one computer to another is known as a:

- A. duplicate chec
- B. table looku
- C. validity chec
- D. parity chec

Answer: D

Explanation:

A parity check will help to detect data errors when data are read from memory or communicated from one computer to another. A one-bit digit (either 0 or 1) is added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, an error report is generated.

NEW QUESTION 9

- (Topic 1)

Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

- A. Paper test
- B. Post test
- C. Preparedness test
- D. Walk-through

Answer: C

Explanation:

A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments.

NEW QUESTION 10

- (Topic 1)

In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

- A. registration authority (RA).
- B. issuing certification authority (CA).
- C. subject C
- D. policy management authorit

Answer: A

Explanation:

A RA is an entity that is responsible for identification and authentication of certificate subjects, but the RA does not sign or issue certificates. The certificate subject usually interacts with the RA for completing the process of subscribing to the services of the certification authority in terms of getting identity validated with standard identification documents, as detailed in the certificate policies of the CA. In the context of a particular certificate, the issuing CA is the CA that issued the certificate. In the context of a particular CA certificate, the subject CA is the CA whose public key is certified in the certificate.

NEW QUESTION 10

- (Topic 1)

What is the PRIMARY purpose of audit trails?

- A. To document auditing efforts
- B. To correct data integrity errors
- C. To establish accountability and responsibility for processed transactions
- D. To prevent unauthorized access to data

Answer: C

Explanation:

The primary purpose of audit trails is to establish accountability and responsibility for processed transactions.

NEW QUESTION 14

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 19

- (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 20

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 21

- (Topic 1)

An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

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

Answer: A

Explanation:

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

NEW QUESTION 23

- (Topic 1)

What is the most common purpose of a virtual private network implementation?

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

Answer: A

Explanation:

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

NEW QUESTION 26

- (Topic 1)

Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

- A. Concurrency controls
- B. Reasonableness checks
- C. Time stamps
- D. Referential integrity controls

Answer: C

Explanation:

Time stamps are an effective control for detecting duplicate transactions such as payments made or received.

NEW QUESTION 27

- (Topic 1)

Which of the following is a guiding best practice for implementing logical access controls?

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

Answer: B

Explanation:

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

NEW QUESTION 28

- (Topic 1)

Which of the following is an effective method for controlling downloading of files via FTP? Choose the BEST answer.

- A. An application-layer gateway, or proxy firewall, but not stateful inspection firewalls
- B. An application-layer gateway, or proxy firewall
- C. A circuit-level gateway
- D. A first-generation packet-filtering firewall

Answer: B

Explanation:

Application-layer gateways, or proxy firewalls, are an effective method for controlling downloading of files via FTP. Because FTP is an OSI application-layer protocol, the most effective firewall needs to be capable of inspecting through the application layer.

NEW QUESTION 33

- (Topic 1)

Which of the following is BEST characterized by unauthorized modification of data before or during systems data entry?

- A. Data diddling
- B. Skimming
- C. Data corruption
- D. Salami attack

Answer: A

Explanation:

Data diddling involves modifying data before or during systems data entry.

NEW QUESTION 38

- (Topic 1)

Which of the following is MOST critical during the business impact assessment phase of business continuity planning?

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

Answer: A

Explanation:

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

NEW QUESTION 39

- (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 44

- (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 45

- (Topic 1)

What influences decisions regarding criticality of assets?

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

Answer: C

Explanation:

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

NEW QUESTION 49

- (Topic 1)

Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

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

Answer: A

Explanation:

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

NEW QUESTION 53

- (Topic 1)

With the objective of mitigating the risk and impact of a major business interruption, a disaster recovery plan should endeavor to reduce the length of recovery time necessary, as well as costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs. True or false?

- A. True
- B. False

Answer: A

Explanation:

With the objective of mitigating the risk and impact of a major business interruption, a disaster-recovery plan should endeavor to reduce the length of recovery time necessary and the costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs.

NEW QUESTION 56

- (Topic 1)

Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

- A. True
- B. False

Answer: A

Explanation:

Obtaining user approval of program changes is very effective for controlling application changes and maintenance.

NEW QUESTION 57

- (Topic 1)

Library control software restricts source code to:

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

Answer: A

Explanation:

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

NEW QUESTION 62

- (Topic 1)

When is regression testing used to determine whether new application changes have introduced any errors in the remaining unchanged code?

- A. In program development and change management
- B. In program feasibility studies
- C. In program development
- D. In change management

Answer: A

Explanation:

Regression testing is used in program development and change management to determine whether new changes have introduced any errors in the remaining unchanged code.

NEW QUESTION 63

- (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 67

- (Topic 1)

Whenever an application is modified, what should be tested to determine the full impact of the change? Choose the BEST answer.

- A. Interface systems with other applications or systems
- B. The entire program, including any interface systems with other applications or systems
- C. All programs, including interface systems with other applications or systems
- D. Mission-critical functions and any interface systems with other applications or systems

Answer: B

Explanation:

Whenever an application is modified, the entire program, including any interface systems with other applications or systems, should be tested to determine the full impact of the change.

NEW QUESTION 70

- (Topic 1)

Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

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

Answer: D

Explanation:

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

NEW QUESTION 74

- (Topic 1)

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do? Choose the BEST answer.

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

Answer: C

Explanation:

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

NEW QUESTION 78

- (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 80

- (Topic 1)

A transaction journal provides the information necessary for detecting unauthorized _____ (fill in the blank) from a terminal.

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

Answer: B

Explanation:

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

NEW QUESTION 85

- (Topic 1)

Parity bits are a control used to validate:

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

Answer: B

Explanation:

Parity bits are a control used to validate data completeness.

NEW QUESTION 89

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 90

- (Topic 1)

What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

- A. Document existing internal controls
- B. Perform compliance testing on internal controls
- C. Establish a controls-monitoring steering committee
- D. Identify high-risk areas within the organization

Answer: D

Explanation:

When implementing continuous-monitoring systems, an IS auditor's first step is to identify highrisk areas within the organization.

NEW QUESTION 95

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 100

- (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 101

- (Topic 1)

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

- A. To advise senior management
- B. To reassign job functions to eliminate potential fraud
- C. To implement compensating control
- D. Segregation of duties is an administrative control not considered by an IS auditor

Answer: A

Explanation:

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

NEW QUESTION 102

- (Topic 1)

When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered. The auditor should especially focus on procedures in an audit of IS strategy. True or false?

- A. True
- B. False

Answer: B

Explanation:

When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered.

NEW QUESTION 103

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 105

- (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 109

- (Topic 1)

When reviewing print systems spooling, an IS auditor is MOST concerned with which of the following vulnerabilities?

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

Answer: C

Explanation:

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

NEW QUESTION 114

- (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 traffic
- 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 117

- (Topic 1)

How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

- A. Modems convert analog transmissions to digital, and digital transmission to analog
- B. Modems encapsulate analog transmissions within digital, and digital transmissions within analog
- C. Modems convert digital transmissions to analog, and analog transmissions to digital
- D. Modems encapsulate digital transmissions within analog, and analog transmissions within digital

Answer: A

Explanation:

Modems (modulation/demodulation) convert analog transmissions to digital, and digital transmissions to analog, and are required for analog transmissions to enter a digital network.

NEW QUESTION 120

- (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 123

- (Topic 1)

What are trojan horse programs? Choose the BEST answer.

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

Answer: D

Explanation:

Trojan horse programs are a common form of Internet attack.

NEW QUESTION 128

- (Topic 1)

Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

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

Answer: A

Explanation:

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

NEW QUESTION 133

- (Topic 1)

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

- A. False
- B. True

Answer: B

Explanation:

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

NEW QUESTION 135

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 136

- (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 138

- (Topic 1)

What determines the strength of a secret key within a symmetric key cryptosystem?

- A. A combination of key length, degree of permutation, and the complexity of the data-encryption algorithm that uses the key
- B. A combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key
- C. A combination of key length and the complexity of the data-encryption algorithm that uses the key
- D. Initial input vectors and the complexity of the data-encryption algorithm that uses the key

Answer: B

Explanation:

The strength of a secret key within a symmetric key cryptosystem is determined by a combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key.

NEW QUESTION 143

- (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 146

- (Topic 1)

Rather than simply reviewing the adequacy of access control, appropriateness of access policies, and effectiveness of safeguards and procedures, the IS auditor is more concerned with effectiveness and utilization of assets. True or false?

- A. True
- B. False

Answer: B

Explanation:

Instead of simply reviewing the effectiveness and utilization of assets, an IS auditor is more concerned with adequate access control, appropriate access policies, and effectiveness of safeguards and procedures.

NEW QUESTION 148

- (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 153

- (Topic 1)

Mitigating the risk and impact of a disaster or business interruption usually takes priority over transference of risk to a third party such as an insurer. True or false?

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 158

- (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 159

- (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 163

- (Topic 1)

Who is responsible for the overall direction, costs, and timetables for systems-development projects?

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

Answer: B

Explanation:

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

NEW QUESTION 164

- (Topic 1)

When should plans for testing for user acceptance be prepared? Choose the BEST answer.

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

Answer: A

Explanation:

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

NEW QUESTION 165

- (Topic 1)

Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

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

Answer: A

Explanation:

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

NEW QUESTION 167

- (Topic 1)

Input/output controls should be implemented for which applications in an integrated systems environment?

- A. The receiving application
- B. The sending application
- C. Both the sending and receiving applications
- D. Output on the sending application and input on the receiving application

Answer: C

Explanation:

Input/output controls should be implemented for both the sending and receiving applications in an integrated systems environment

NEW QUESTION 171

- (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 172

- (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 173

- (Topic 2)

The PRIMARY purpose of audit trails is to:

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

Answer: B

Explanation:

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

NEW QUESTION 176

- (Topic 2)

To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

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

Answer: C

Explanation:

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

NEW QUESTION 181

- (Topic 2)

While planning an audit, an assessment of risk should be made to provide:

- A. reasonable assurance that the audit will cover material items
- B. definite assurance that material items will be covered during the audit work
- C. reasonable assurance that all items will be covered by the audit
- D. sufficient assurance that all items will be covered during the audit work

Answer: A

Explanation:

The ISACA IS Auditing Guideline G15 on planning the IS audit states, 'An assessment of risk should be made to provide reasonable assurance that material items will be adequately covered during the audit work. This assessment should identify areas with a relatively high risk of the existence of material problems.' Definite assurance that material items will be covered during the audit work is an impractical proposition. Reasonable assurance that all items will be covered during the audit work is not the correct answer, as material items need to be covered, not all items.

NEW QUESTION 186

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 190

- (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 192

- (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 193

- (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 194

- (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 199

- (Topic 2)

Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

- A. Discussion with management
- B. Review of the organization chart
- C. Observation and interviews
- D. Testing of user access rights

Answer: C

Explanation:

By observing the IS staff performing their tasks, an IS auditor can identify whether they are performing any incompatible operations, and by interviewing the IS staff, the auditor can get an overview of the tasks performed. Based on the observations and interviews the auditor can evaluate the segregation of duties. Management may not be aware of the detailed functions of each employee in the IS department; therefore, discussion with the management would provide only limited information regarding segregation of duties. An organization chart would not provide details of the functions of the employees. Testing of user rights would provide information about the rights they have within the IS systems, but would not provide complete information about the functions they perform.

NEW QUESTION 202

- (Topic 2)

Which of the following would be the BEST population to take a sample from when testing program changes?

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

Answer: D

Explanation:

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

executables.

NEW QUESTION 207

- (Topic 2)

Data flow diagrams are used by IS auditors to:

- A. order data hierarchicall
- B. highlight high-level data definition
- C. graphically summarize data paths and storag
- D. portray step-by-step details of data generatio

Answer: C

Explanation:

Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of data. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

NEW QUESTION 208

- (Topic 2)

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

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

Answer: C

Explanation:

An IS auditor should next examine cases where incorrect calculations occurred and confirm the results. After the calculations have been confirmed, further tests can be conducted and reviewed. Report preparation, findings and recommendations would not be made until all results are confirmed.

NEW QUESTION 211

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 212

- (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 mechanis
- B. Clear the virus from the networ
- C. Inform appropriate personnel immediatel
- D. Ensure deletion of the viru

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 217

- (Topic 2)

The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

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

Answer: B

Explanation:

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

NEW QUESTION 222

- (Topic 2)

During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

- A. Dumping the memory content to a file
- B. Generating disk images of the compromised system
- C. Rebooting the system
- D. Removing the system from the network

Answer: C

Explanation:

Rebooting the system may result in a change in the system state and the loss of files and important evidence stored in memory. The other choices are appropriate actions for preserving evidence.

NEW QUESTION 223

- (Topic 2)

An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

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

Answer: C

Explanation:

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

NEW QUESTION 228

- (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 mediates 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 230

- (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 231

- (Topic 3)

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

- A. IT budge
- B. existing IT environmen
- C. business pla
- D. investment pla

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 233

- (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 236

- (Topic 3)

Responsibility for the governance of IT should rest with the:

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

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 238

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 243

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 246

- (Topic 3)

When an employee is terminated from service, the MOST important action is to:

- A. hand over all of the employee's files to another designated employee
- B. complete a backup of the employee's work
- C. notify other employees of the termination
- D. disable the employee's logical access

Answer: D

Explanation:

There is a probability that a terminated employee may misuse access rights; therefore, disabling the terminated employee's logical access is the most important action to take. All the work of the terminated employee needs to be handed over to a designated employee; however, this should be performed after implementing choice D. All the work of the terminated employee needs to be backed up and the employees need to be notified of the termination of the employee, but this should not precede the action in choice D.

NEW QUESTION 249

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 253

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 255

- (Topic 3)

Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

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

Answer: D

Explanation:

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness that may arise when duties cannot be appropriately segregated. Overlapping controls are two controls addressing the same control objective or exposure. Since primary controls cannot be achieved when duties cannot or are not appropriately segregated, it is difficult to install overlapping controls. Boundary controls establish the interface between the would-be

user of a computer system and the computer system itself, and are individual-based, not role-based, controls. Access controls for resources are based on individuals and not on roles.

NEW QUESTION 257

- (Topic 3)

Which of the following is a risk of cross-training?

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

Answer: C

Explanation:

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

NEW QUESTION 260

- (Topic 3)

Which of the following is normally a responsibility of the chief security officer (CSO)?

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

Answer: A

Explanation:

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

NEW QUESTION 261

- (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 266

- (Topic 3)

Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

- A. User management coordination does not exis
- B. Specific user accountability cannot be establishe
- C. Unauthorized users may have access to originate, modify or delete dat
- D. Audit recommendations may not be implemente

Answer: C

Explanation:

Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

NEW QUESTION 269

- (Topic 3)

The PRIMARY objective of an audit of IT security policies is to ensure that:

- A. they are distributed and available to all staf
- B. security and control policies support business and IT objective

- C. there is a published organizational chart with functional description
- D. duties are appropriately segregate

Answer: B

Explanation:

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

NEW QUESTION 270

- (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 271

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 272

- (Topic 3)

Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

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

Answer: C

Explanation:

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

NEW QUESTION 274

- (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 278

- (Topic 3)

Which of the following provides the best evidence of the adequacy of a security awareness program?

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

Answer: D

Explanation:

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

NEW QUESTION 279

- (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 280

- (Topic 3)

An example of a direct benefit to be derived from a proposed IT-related business investment is:

- A. enhanced reputatio
- B. enhanced staff moral
- C. the use of new technolog
- D. increased market penetratio

Answer: D

Explanation:

A comprehensive business case for any proposed IT-related business investment should have clearly defined business benefits to enable the expected return to be calculated. These benefits usually fall into two categories: direct and indirect, or soft. Direct benefits usually comprise the quantifiable financial benefits that the new system is expected to generate. The potential benefits of enhanced reputation and enhanced staff morale are difficult to quantify, but should be quantified to the extent possible. IT investments should not be made just for the sake of new technology but should be based on a quantifiable business need.

NEW QUESTION 282

- (Topic 3)

When an organization is outsourcing their information security function, which of the following should be kept in the organization?

- A. Accountability for the corporate security policy
- B. Defining the corporate security policy
- C. Implementing the corporate security policy
- D. Defining security procedures and guidelines

Answer: A

Explanation:

Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

NEW QUESTION 283

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 284

- (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 285

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 286

- (Topic 3)

A poor choice of passwords and transmission over unprotected communications lines are examples of:

- A. vulnerabilitie
- B. threat
- C. probabilitie
- D. impact

Answer: A

Explanation:

Vulnerabilities represent characteristics of information resources that may be exploited by a threat. Threats are circumstances or events with the potential to cause harm to information resources. Probabilities represent the likelihood of the occurrence of a threat, while impacts represent the outcome or result of a threat exploiting a vulnerability.

NEW QUESTION 287

- (Topic 4)

To minimize the cost of a software project, quality management techniques should be applied:

- A. as close to their writing (i.e., point of origination) as possibl
- B. primarily at project start-up to ensure that the project is established in accordance with organizational governance standard
- C. continuously throughout the project with an emphasis on finding and fixing defects primarily during testing to maximize the defect detection rat
- D. mainly at project close-down to capture lessons learned that can be applied to future project

Answer: C

Explanation:

While it is important to properly establish a software development project, quality management should be effectively practiced throughout the project. The major source of unexpected costs on most software projects is rework. The general rule is thatthe earlier in the development life cycle that a defect occurs, and the longer it takes to find and fix that defect, the more effort will be needed to correct it. A well-written quality management plan is a good start, but it must also be

actively applied. Simply relying on testing to identify defects is a relatively costly and less effective way of achieving software quality. For example, an error in requirements discovered in the testing phase can result in scrapping significant amounts of work. Capturing lessons learned will be too late for the current project. Additionally, applying quality management techniques throughout a project is likely to yield its own insights into the causes of quality problems and assist in staff development.

NEW QUESTION 288

- (Topic 4)

While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

- A. effectiveness of the QA function because it should interact between project management and user management
- B. efficiency of the QA function because it should interact with the project implementation team
- C. effectiveness of the project manager because the project manager should interact with the QA function
- D. efficiency of the project manager because the QA function will need to communicate with the project implementation team

Answer: A

Explanation:

To be effective the quality assurance (QA) function should be independent of project management. The QA function should never interact with the project implementation team since this can impact effectiveness. The project manager does not interact with the QA function, which should not impact the effectiveness of the project manager. The QA function does not interact with the project implementation team, which should not impact the efficiency of the project manager.

NEW QUESTION 291

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 296

- (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 299

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 300

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 305

- (Topic 4)

Which of the following techniques would BEST help an IS auditor gain reasonable assurance that a project can meet its target date?

- A. Estimation of the actual end date based on the completion percentages and estimated time to complete, taken from status reports
- B. Confirmation of the target date based on interviews with experienced managers and staff involved in the completion of the project deliverables
- C. Extrapolation of the overall end date based on completed work packages and current resources
- D. Calculation of the expected end date based on current resources and remaining available project budget

Answer: C

Explanation:

Direct observation of results is better than estimations and qualitative information gained from interviews or status reports. Project managers and involved staff tend to underestimate the time needed for completion and the necessary time buffers for dependencies between tasks, while overestimating the completion percentage for tasks underway (80:20 rule). The calculation based on remaining budget does not take into account the speed at which the project has been progressing.

NEW QUESTION 308

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 313

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 316

- (Topic 4)

Information for detecting unauthorized input from a terminal would be BEST provided by the:

- A. console log printout
- B. transaction journal
- C. automated suspense file listing
- D. user error report

Answer: B

Explanation:

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

NEW QUESTION 319

- (Topic 4)

Functional acknowledgements are used:

- A. as an audit trail for EDI transaction
- B. to functionally describe the IS department
- C. to document user roles and responsibilities
- D. as a functional description of application software

Answer: A

Explanation:

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

NEW QUESTION 322

- (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 327

- (Topic 4)

What control detects transmission errors by appending calculated bits onto the end of each segment of data?

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

Answer: C

Explanation:

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

NEW QUESTION 329

- (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 331

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 335

- (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 336

- (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 338

- (Topic 4)

Ideally, stress testing should be carried out in a:

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

Answer: C

Explanation:

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

NEW QUESTION 342

- (Topic 4)

The phases and deliverables of a system development life cycle (SDLC) project should be determined:

- A. during the initial planning stages of the projec

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

Answer: A

Explanation:

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

NEW QUESTION 347

- (Topic 4)

A decision support system (DSS):

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

Answer: C

Explanation:

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

NEW QUESTION 351

- (Topic 4)

An advantage of using sanitized live transactions in test data is that:

- A. all transaction types will be included
- B. every error condition is likely to be tested
- C. no special routines are required to assess the result
- D. test transactions are representative of live processing

Answer: D

Explanation:

Test data will be representative of live processing; however, it is unlikely that all transaction types or error conditions will be tested in this way.

NEW QUESTION 355

- (Topic 4)

An advantage in using a bottom-up vs. a top-down approach to software testing is that:

- A. interface errors are detected earlier
- B. confidence in the system is achieved earlier
- C. errors in critical modules are detected earlier
- D. major functions and processing are tested earlier

Answer: C

Explanation:

The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and works upward until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices in this question all refer to advantages of a top-down approach, which follows the opposite path, either in depth-first or breadth-first search order.

NEW QUESTION 359

- (Topic 4)

During which of the following phases in system development would user acceptance test plans normally be prepared?

- A. Feasibility study
- B. Requirements definition
- C. implementation planning
- D. Postimplementation review

Answer: B

Explanation:

During requirements definition, the project team will be working with the users to define their precise objectives and functional needs. At this time, the users should be working with the team to consider and document how the system functionality can be tested to ensure it meets their stated needs. The feasibility study is too early for such detailed user involvement, and the implementation planning and postimplementation review phases are too late. An IS auditor should know at what point user testing should be planned to ensure it is most effective and efficient.

NEW QUESTION 360

- (Topic 4)

Which of the following should be included in a feasibility study for a project to implement an EDI process?

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

Answer: C

Explanation:

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

NEW QUESTION 365

- (Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 368

- (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 371

- (Topic 4)

The waterfall life cycle model of software development is most appropriately used when:

- A. requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate
- B. requirements are well understood and the project is subject to time pressure
- C. the project intends to apply an object-oriented design and programming approach
- D. the project will involve the use of new technology

Answer: A

Explanation:

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

NEW QUESTION 375

- (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 378

- (Topic 4)

Which of the following is an advantage of the top-down approach to software testing?

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

Answer: A

Explanation:

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

NEW QUESTION 379

- (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 383

- (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 387

- (Topic 4)

Which of the following would help to ensure the portability of an application connected to a database?

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

Answer: B

Explanation:

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

portability of an application connecting to a database.

NEW QUESTION 388

- (Topic 4)

Business units are concerned about the performance of a newly implemented system. Which of the following should an IS auditor recommend?

- A. Develop a baseline and monitor system usage
- B. Define alternate processing procedure
- C. Prepare the maintenance manual
- D. Implement the changes users have suggested

Answer: A

Explanation:

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

NEW QUESTION 393

- (Topic 4)

An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:

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

Answer: C

Explanation:

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

NEW QUESTION 397

- (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 type
- B. verify the format of the number entered then locate it on the database
- C. ensure that the transaction entered is within the cardholder's credit limit
- D. confirm that the card is not shown as lost or stolen on the master file

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 398

- (Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 403

- (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 manually

- 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 405

- (Topic 4)

When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?

- A. Use of a cryptographic hashing algorithm
- B. Enciphering the message digest
- C. Deciphering the message digest
- D. A sequence number and time stamp

Answer: D

Explanation:

When transmitting data, a sequence number and/or time stamp built into the message to make it unique can be checked by the recipient to ensure that the message was not intercepted and replayed. This is known as replay protection, and could be used to verify that a payment instruction was not duplicated. Use of a cryptographic hashing algorithm against the entire message helps achieve data integrity. Enciphering the message digest using the sender's private key, which signs the sender's digital signature to the document, helps in authenticating the transaction. When the message is deciphered by the receiver using the sender's public key, it ensures that the message could only have come from the sender. This process of sender authentication achieves nonrepudiation.

NEW QUESTION 408

- (Topic 4)

When using an integrated test facility (ITF), an IS auditor should ensure that:

- A. production data are used for testing
- B. test data are isolated from production data
- C. a test data generator is used
- D. master files are updated with the test data

Answer: B

Explanation:

An integrated test facility (ITF) creates a fictitious file in the database, allowing for test transactions to be processed simultaneously with live data. While this ensures that periodic testing does not require a separate test process, there is a need to isolate test data from production data. An IS auditor is not required to use production data or a test data generator. Production master files should not be updated with test data.

NEW QUESTION 410

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 411

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 414

- (Topic 5)

Which of the following reports should an IS auditor use to check compliance with a service level agreement's (SLA) requirement for uptime?

- A. Utilization reports
- B. Hardware error reports
- C. System logs
- D. Availability reports

Answer: D

Explanation:

IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment, and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. System logs are a recording of the system's activities.

NEW QUESTION 419

- (Topic 5)

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

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

Answer: B

Explanation:

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

NEW QUESTION 420

- (Topic 5)

To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?

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

Answer: D

Explanation:

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

NEW QUESTION 422

- (Topic 5)

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

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

Answer: A

Explanation:

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

NEW QUESTION 423

- (Topic 5)

Which of the following BEST ensures the integrity of a server's operating system?

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

Answer: C

Explanation:

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

NEW QUESTION 424

- (Topic 5)

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

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

Answer: C

Explanation:

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

NEW QUESTION 428

- (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 accesses
- 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 433

- (Topic 5)

Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:

- A. protect the organization from viruses and nonbusiness material
- B. maximize employee performance
- C. safeguard the organization's image
- D. assist the organization in preventing legal issues

Answer: A

Explanation:

The main reason for investing in web and e-mail filtering tools is that they significantly reduce risks related to viruses, spam, mail chains, recreational surfing and recreational e-mail. Choice B could be true in some circumstances (i.e., it would need to be implemented along with an awareness program, so that employee performance can be significantly improved). However, in such cases, it would not be as relevant as choice A. Choices C and D are secondary or indirect benefits.

NEW QUESTION 438

- (Topic 5)

In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

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

Answer: A

Explanation:

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

NEW QUESTION 439

.....

Relate Links

100% Pass Your CISA Exam with Exambible Prep Materials

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

Contact us

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

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