

CISA Dumps

Isaca CISA

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



NEW QUESTION 1

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 2

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 3

- (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 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)

Structured programming is BEST described as a technique that:

- A. provides knowledge of program functions to other programmers via peer review
- B. reduces the maintenance time of programs by the use of small-scale program module
- C. makes the readable coding reflect as closely as possible the dynamic execution of the program

D. controls the coding and testing of the high-level functions of the program in the development proces

Answer: B

Explanation:

A characteristic of structured programming is smaller, workable units. Structured programming has evolved because smaller, workable units are easier to maintain. Structured programming is a style of programming which restricts the kinds of control structures. This limitation is not crippling. Any program can be written with allowed control structures. Structured programming is sometimes referred to as go-to-less programming, since a go-to statement is not allowed. This is perhaps the most well known restriction of the style, since go-to statements were common at the time structured programming was becoming more popular. Statement labels also become unnecessary, except in languages where subroutines are identified by labels.

NEW QUESTION 6

- (Topic 1)

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

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

Answer: B

Explanation:

A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted. This control is effective in detecting transposition and transcription errors.

NEW QUESTION 7

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 8

- (Topic 1)

The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

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

Answer: D

Explanation:

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

NEW QUESTION 9

- (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 10

- (Topic 1)

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

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

Answer: C

Explanation:

A completeness check is used to determine if a field contains data and not zeros or blanks.

NEW QUESTION 10

- (Topic 1)

A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

- A. digest signatur
- B. electronic signatur
- C. digital signatur
- D. hash signatur

Answer: C

Explanation:

A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. It is a string of bits that uniquely represent another string of bits, a digital document. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad, connected to the system.

NEW QUESTION 14

- (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 18

- (Topic 1)

Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

- A. Specific developments only
- B. Business requirements only
- C. All phases of the installation must be documented
- D. No need to develop a customer specific documentation

Answer: C

Explanation:

A global enterprise product reengineering (EPR) software package can be applied to a business to replace, simplify and improve the quality of IS processing. Documentation is intended to help understand how, why and which solutions that have been selected and implemented, and therefore must be specific to the project. Documentation is also intended to support quality assurance and must be comprehensive.

NEW QUESTION 23

- (Topic 1)

What is the primary objective of a control self-assessment (CSA) program?

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

Answer: A

Explanation:

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

NEW QUESTION 24

- (Topic 1)

As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

- A. The same value
- B. Greater value
- C. Lesser value
- D. Prior audit reports are not relevant

Answer: C

Explanation:

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

NEW QUESTION 29

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 31

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 32

- (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 36

- (Topic 1)

If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

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

Answer: C

Explanation:

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

NEW QUESTION 37

- (Topic 1)

What would an IS auditor expect to find in the console log? Choose the BEST answer.

- A. Evidence of password spoofing

- B. System errors
- C. Evidence of data copy activities
- D. Evidence of password sharing

Answer: B

Explanation:

An IS auditor can expect to find system errors to be detailed in the console log.

NEW QUESTION 40

- (Topic 1)

Why does the IS auditor often review the system logs?

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

Answer: C

Explanation:

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

NEW QUESTION 42

- (Topic 1)

What is essential for the IS auditor to obtain a clear understanding of network management?

- A. Security administrator access to systems
- B. Systems logs of all hosts providing application services
- C. A graphical map of the network topology
- D. Administrator access to systems

Answer: C

Explanation:

A graphical interface to the map of the network topology is essential for the IS auditor to obtain a clear understanding of network management.

NEW QUESTION 47

- (Topic 1)

What can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program? Choose the BEST answer.

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

Answer: B

Explanation:

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

NEW QUESTION 48

- (Topic 1)

What increases encryption overhead and cost the most?

- A. A long symmetric encryption key
- B. A long asymmetric encryption key
- C. A long Advance Encryption Standard (AES) key
- D. A long Data Encryption Standard (DES) key

Answer: B

Explanation:

A long asymmetric encryption key (public key encryption) increases encryption overhead and cost. All other answers are single shared symmetric keys.

NEW QUESTION 51

- (Topic 1)

Which of the following best characterizes "worms"?

- A. Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
- B. Programming code errors that cause a program to repeatedly dump data
- C. Malicious programs that require the aid of a carrier program such as email
- D. Malicious programs that masquerade as common applications such as screensavers or macro-enabled Word documents

Answer: A

Explanation:

Worms are malicious programs that can run independently and can propagate without the aid of a carrier program such as email.

NEW QUESTION 56

- (Topic 1)

Which of the following do digital signatures provide?

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

Answer: A

Explanation:

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

NEW QUESTION 60

- (Topic 1)

Which of the following would provide the highest degree of server access control?

- A. A mantrap-monitored entryway to the server room
- B. Host-based intrusion detection combined with CCTV
- C. Network-based intrusion detection
- D. A fingerprint scanner facilitating biometric access control

Answer: D

Explanation:

A fingerprint scanner facilitating biometric access control can provide a very high degree of server access control.

NEW QUESTION 63

- (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 68

- (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 73

- (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 77

- (Topic 1)

Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

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

Answer: C

Explanation:

Of the three major types of BCP tests (paper, walk-through, and preparedness), a walk-through test requires only that representatives from each operational area meet to review the plan.

NEW QUESTION 80

- (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 85

- (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 87

- (Topic 1)

Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

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

Answer: A

Explanation:

A cold site is often an acceptable solution for preparing for recovery of noncritical systems and data.

NEW QUESTION 90

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 95

- (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 96

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 97

- (Topic 1)

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

- A. True
- B. False

Answer: B

Explanation:

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

NEW QUESTION 99

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 104

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 109

- (Topic 1)

What is the first step in a business process re-engineering project?

- A. Identifying current business processes
- B. Forming a BPR steering committee
- C. Defining the scope of areas to be reviewed
- D. Reviewing the organizational strategic plan

Answer: C

Explanation:

Defining the scope of areas to be reviewed is the first step in a business process re-engineering project.

NEW QUESTION 110

- (Topic 1)

When are benchmarking partners identified within the benchmarking process?

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

Answer: C

Explanation:

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

NEW QUESTION 114

- (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 115

- (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 120

- (Topic 1)

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

- A. Text search forensic utility software
- B. Generalized audit software
- C. Productivity audit software
- D. Manual review

Answer: B

Explanation:

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

NEW QUESTION 125

- (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 128

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 131

- (Topic 1)

Ensuring that security and control policies support business and IT objectives is a primary objective of:

- A. An IT security policies audit
- B. A processing audit
- C. A software audit
- D. A vulnerability assessment

Answer: A

Explanation:

Ensuring that security and control policies support business and IT objectives is a primary objective of an IT security policies audit.

NEW QUESTION 136

- (Topic 1)

When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

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

Answer: A

Explanation:

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

NEW QUESTION 140

- (Topic 1)

Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 141

- (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 146

- (Topic 1)

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

- A. Risk varies
- B. Risk is reduced
- C. Risk is not affected
- D. Risk is increased

Answer: D

Explanation:

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

NEW QUESTION 148

- (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 151

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 152

- (Topic 1)

What type(s) of firewalls provide(s) the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic?

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

Answer: C

Explanation:

An application-layer gateway, or proxy firewall, and stateful-inspection firewalls provide the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic.

NEW QUESTION 153

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 157

- (Topic 1)

What is/are used to measure and ensure proper network capacity management and availability of services? Choose the BEST answer.

- A. Network performance-monitoring tools
- B. Network component redundancy
- C. Syslog reporting
- D. IT strategic planning

Answer: A

Explanation:

Network performance-monitoring tools are used to measure and ensure proper network capacity management and availability of services.

NEW QUESTION 161

- (Topic 1)

Which of the following fire-suppression methods is considered to be the most environmentally friendly?

- A. Halon gas
- B. Deluge sprinklers
- C. Dry-pipe sprinklers

D. Wet-pipe sprinklers

Answer: C

Explanation:

Although many methods of fire suppression exist, dry-pipe sprinklers are considered to be the most environmentally friendly.

NEW QUESTION 166

- (Topic 1)

What type of fire-suppression system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities?

- A. A dry-pipe sprinkler system
- B. A deluge sprinkler system
- C. A wet-pipe system
- D. A halon sprinkler system

Answer: A

Explanation:

A dry-pipe sprinkler system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities.

NEW QUESTION 171

- (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 172

- (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 177

- (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 181

- (Topic 1)

What process is used to validate a subject's identity?

- A. Identification
- B. Nonrepudiation
- C. Authorization
- D. Authentication

Answer: D

Explanation:

Authentication is used to validate a subject's identity.

NEW QUESTION 186

- (Topic 1)

What should IS auditors always check when auditing password files?

- A. That deleting password files is protected
- B. That password files are encrypted
- C. That password files are not accessible over the network
- D. That password files are archived

Answer: B

Explanation:

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

NEW QUESTION 189

- (Topic 1)

Which of the following is the most fundamental step in preventing virus attacks?

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

Answer: A

Explanation:

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

NEW QUESTION 192

- (Topic 1)

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 197

- (Topic 1)

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

- A. True
- B. False

Answer: B

Explanation:

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

NEW QUESTION 200

- (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 202

- (Topic 1)

Off-site data backup and storage should be geographically separated so as to _____ (fill in the blank) the risk of a widespread physical disaster such

as a hurricane or earthquake.

- A. Accept
- B. Eliminate
- C. Transfer
- D. Mitigate

Answer: D

Explanation:

Off-site data backup and storage should be geographically separated, to mitigate the risk of a widespread physical disaster such as a hurricane or an earthquake.

NEW QUESTION 207

- (Topic 1)

What uses questionnaires to lead the user through a series of choices to reach a conclusion? Choose the BEST answer.

- A. Logic trees
- B. Decision trees
- C. Decision algorithms
- D. Logic algorithms

Answer: B

Explanation:

Decision trees use questionnaires to lead the user through a series of choices to reach a conclusion.

NEW QUESTION 211

- (Topic 1)

Who is ultimately responsible for providing requirement specifications to the software-development team?

- A. The project sponsor
- B. The project members
- C. The project leader
- D. The project steering committee

Answer: A

Explanation:

The project sponsor is ultimately responsible for providing requirement specifications to the software-development team.

NEW QUESTION 213

- (Topic 1)

What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?

- A. Contrived data
- B. Independently created data
- C. Live data
- D. Data from previous tests

Answer: D

Explanation:

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

NEW QUESTION 217

- (Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 219

- (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 224

- (Topic 1)

What kind of testing should programmers perform following any changes to an application or system?

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

Answer: A

Explanation:

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

NEW QUESTION 226

- (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 230

- (Topic 1)

After identifying potential security vulnerabilities, what should be the IS auditor's next step?

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

Answer: C

Explanation:

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

NEW QUESTION 233

- (Topic 1)

Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?

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

Answer: B

Explanation:

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

NEW QUESTION 237

- (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 241

- (Topic 1)

What is used as a control to detect loss, corruption, or duplication of data?

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

Answer: C

Explanation:

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

NEW QUESTION 245

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 250

- (Topic 1)

Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

- A. True
- B. False

Answer: A

Explanation:

Database snapshots can provide an excellent audit trail for an IS auditor.

NEW QUESTION 255

- (Topic 2)

An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

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

Answer: C

Explanation:

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

NEW QUESTION 260

- (Topic 2)

Which of the following is a benefit of a risk-based approach to audit planning? Audit:

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

Answer: D

Explanation:

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

NEW QUESTION 263

- (Topic 2)

The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

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

Answer: C

Explanation:

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

NEW QUESTION 267

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 269

- (Topic 2)

An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

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

Answer: D

Explanation:

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

NEW QUESTION 272

- (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 275

- (Topic 2)

Which of the following forms of evidence for the auditor would be considered the MOST reliable?

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

Answer: D

Explanation:

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

NEW QUESTION 277

- (Topic 2)

An IS auditor reviews an organizational chart PRIMARILY for:

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

Answer: C

Explanation:

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

NEW QUESTION 282

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 283

- (Topic 2)

An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

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

Answer: B

Explanation:

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

NEW QUESTION 285

- (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 288

- (Topic 2)

Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

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

Answer: D

Explanation:

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

NEW QUESTION 289

- (Topic 2)

When assessing the design of network monitoring controls, an IS auditor should FIRST review network:

- A. topology diagram
- B. bandwidth usage
- C. traffic analysis report
- D. bottleneck location

Answer: A

Explanation:

The first step in assessing network monitoring controls should be the review of the adequacy of network documentation, specifically topology diagrams. If this information is not up to date, then monitoring processes and the ability to diagnose problems will not be effective.

NEW QUESTION 293

- (Topic 2)

When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

- A. analysis
- B. evaluation
- C. preservation
- D. disclosure

Answer: C

Explanation:

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

NEW QUESTION 294

- (Topic 2)

An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

- A. conclude that the controls are inadequate
- B. expand the scope to include substantive testing
- C. place greater reliance on previous audit
- D. suspend the audit

Answer: B

Explanation:

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

NEW QUESTION 297

- (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 301

- (Topic 2)

Which of the following should an IS auditor use to detect duplicate invoice records within an invoice master file?

- A. Attribute sampling
- B. Generalized audit software (GAS)
- C. Test data
- D. Integrated test facility (ITF)

Answer: B**Explanation:**

Generalized audit software (GAS) would enable the auditor to review the entire invoice file to look for those items that meet the selection criteria. Attribute sampling would aid in identifying records meeting specific conditions, but would not compare one record to another to identify duplicates. To detect duplicate invoice records the IS auditor should check all of the items that meet the criteria and not just a sample of the items. Test data are used to verify program processing, but will not identify duplicate records. An integrated test facility (ITF) allows the IS auditor to test transactions through the production system, but would not compare records to identify duplicates.

NEW QUESTION 305

- (Topic 2)

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

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

Answer: B**Explanation:**

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

NEW QUESTION 310

- (Topic 2)

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

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

Answer: C**Explanation:**

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

NEW QUESTION 312

- (Topic 2)

Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:

- A. include the finding in the final report, because the IS auditor is responsible for an accurate report of all finding
- B. not include the finding in the final report, because the audit report should include only unresolved finding
- C. not include the finding in the final report, because corrective action can be verified by the IS auditor during the audi
- D. include the finding in the closing meeting for discussion purposes onl

Answer: A

Explanation:

Including the finding in the final report is a generally accepted audit practice. If an action is taken after the audit started and before it ended, the audit report should identify the finding and describe the corrective action taken. An audit report should reflect the situation, as it existed at the start of the audit. All corrective actions taken by the auditee should be reported in writing.

NEW QUESTION 314

- (Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 318

- (Topic 2)

A PRIMARY benefit derived from an organization employing control self-assessment (CSA) techniques is that it:

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

Answer: A

Explanation:

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

NEW QUESTION 319

- (Topic 2)

The success of control self-assessment (CSA) highly depends on:

- A. having line managers assume a portion of the responsibility for control monitoring
- B. assigning staff managers the responsibility for building, but not monitoring, controls
- C. the implementation of a stringent control policy and rule-driven controls
- D. the implementation of supervision and the monitoring of controls of assigned duties

Answer: A

Explanation:

The primary objective of a CSA program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional area line managers. The success of a control self-assessment (CSA) program depends on the degree to which line managers assume responsibility for controls- Choices B, C and D are characteristics of a traditional audit approach, not a CSA approach.

NEW QUESTION 322

- (Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 326

- (Topic 3)

The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

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

Answer: C

Explanation:

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

NEW QUESTION 328

- (Topic 3)

Which of the following is a function of an IS steering committee?

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

Answer: C

Explanation:

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

NEW QUESTION 329

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 332

- (Topic 3)

Effective IT governance will ensure that the IT plan is consistent with the organization's:

- A. business plan
- B. audit plan
- C. security plan
- D. investment plan

Answer: A

Explanation:

To govern IT effectively, IT and business should be moving in the same direction, requiring that the IT plans are aligned with an organization's business plans. The audit and investment plans are not part of the IT plan, while the security plan should be at a corporate level.

NEW QUESTION 334

- (Topic 3)

IT governance is PRIMARILY the responsibility of the:

- A. chief executive office
- B. board of director
- C. IT steering committee
- D. audit committee

Answer:

B

Explanation:

IT governance is primarily the responsibility of the executives and shareholders (as represented by the board of directors). The chief executive officer is instrumental in implementing IT governance per the directions of the board of directors. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. The audit committee reports to the board of directors and should monitor the implementation of audit recommendations.

NEW QUESTION 336

- (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 339

- (Topic 3)

Effective IT governance requires organizational structures and processes to ensure that:

- A. the organization's strategies and objectives extend the IT strategy
- B. the business strategy is derived from an IT strategy
- C. IT governance is separate and distinct from the overall governance
- D. the IT strategy extends the organization's strategies and objectives

Answer: D**Explanation:**

Effective IT governance requires that board and executive management extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives, and that the strategy is aligned with business strategy. Choice A is incorrect because it is the IT strategy that extends the organizational objectives, not the opposite. IT governance is not an isolated discipline; it must become an integral part of the overall enterprise governance.

NEW QUESTION 341

- (Topic 3)

The ultimate purpose of IT governance is to:

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

Answer: A**Explanation:**

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

NEW QUESTION 343

- (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 344

- (Topic 3)

Which of the following would BEST provide assurance of the integrity of new staff?

- A. Background screening
- B. References
- C. Bonding
- D. Qualifications listed on a resume

Answer: A

Explanation:

A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a resume may not be accurate.

NEW QUESTION 347

- (Topic 3)

A local area network (LAN) administrator normally would be restricted from:

- A. having end-user responsibilities
- B. reporting to the end-user manager
- C. having programming responsibilities
- D. being responsible for LAN security administration

Answer: C

Explanation:

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

NEW QUESTION 348

- (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 353

- (Topic 3)

Which of the following reduces the potential impact of social engineering attacks?

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

Answer: C

Explanation:

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

NEW QUESTION 354

- (Topic 3)

In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

- A. there is an integration of IS and business staffs within project
- B. there is a clear definition of the IS mission and vision
- C. a strategic information technology planning methodology is in place
- D. the plan correlates business objectives to IS goals and objectives

Answer: A

Explanation:

The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C and D are areas covered by a strategic plan.

NEW QUESTION 356

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 360

- (Topic 3)

The rate of change in technology increases the importance of:

- A. outsourcing the IS functio
- B. implementing and enforcing good processe
- C. hiring personnel willing to make a career within the organizatio
- D. meeting user requirement

Answer: B

Explanation:

Change requires that good change management processes be implemented and enforced. Outsourcing the IS function is not directly related to the rate of technological change. Personnel in a typical IS department are highly qualified and educated; usually they do not feel their jobs are at risk and are prepared to switch jobs frequently. Although meeting user requirements is important, it is not directly related to the rate of technological change in the IS environment.

NEW QUESTION 361

- (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 364

- (Topic 3)

Which of the following is the initial step in creating a firewall policy?

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

Answer: B

Explanation:

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

NEW QUESTION 369

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 371

- (Topic 3)

Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

- A. Assimilation of the framework and intent of a written security policy by all appropriate parties
- B. Management support and approval for the implementation and maintenance of a security policy
- C. Enforcement of security rules by providing punitive actions for any violation of security rules
- D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Answer: A

Explanation:

Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules, is also required, along with the user's education on the importance of security.

NEW QUESTION 373

- (Topic 3)

A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

- A. recover
- B. retention
- C. rebuilding
- D. reuse

Answer: B

Explanation:

Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the official form of classic 'paper' makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

NEW QUESTION 374

- (Topic 3)

A top-down approach to the development of operational policies will help ensure:

- A. that they are consistent across the organization
- B. that they are implemented as a part of risk assessment
- C. compliance with all policies
- D. that they are reviewed periodically

Answer: A

Explanation:

Deriving lower level policies from corporate policies (a top-down approach) aids in ensuring consistency across the organization and consistency with other policies. The bottom-up approach to the development of operational policies is derived as a result of risk assessment. A top-down approach of itself does not ensure compliance and development does not ensure that policies are reviewed.

NEW QUESTION 376

- (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 year
- C. Privacy laws could prevent cross-border flow of information
- 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 377

- (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 378

- (Topic 3)

An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

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

Answer: C

Explanation:

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

NEW QUESTION 379

- (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 384

- (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 385

- (Topic 3)

A benefit of open system architecture is that it:

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

Answer: A

Explanation:

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

NEW QUESTION 390

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 393

- (Topic 3)

Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

- A. Yes, because an IS auditor will evaluate the adequacy of the service bureau's plan and assist their company in implementing a complementary plan
- B. Yes, because based on the plan, an IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contract
- C. No, because the backup to be provided should be specified adequately in the contract
- D. No, because the service bureau's business continuity plan is proprietary information

Answer: A

Explanation:

The primary responsibility of an IS auditor is to assure that the company assets are being safeguarded. This is true even if the assets do not reside on the immediate premises. Reputable service bureaus will have a well-designed and tested business continuity plan.

NEW QUESTION 395

- (Topic 3)

An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

- A. References from other customers
- B. Service level agreement (SLA) template
- C. Maintenance agreement
- D. Conversion plan

Answer: A

Explanation:

An IS auditor should look for an independent verification that the ISP can perform the tasks being contracted for. References from other customers would provide an independent, external review and verification of procedures and processes the ISP follows—issues which would be of concern to an IS auditor. Checking references is a means of obtaining an independent verification that the vendor can perform the services it says it can. A maintenance agreement relates more to equipment than to services, and a conversion plan, while important, is less important than verification that the ISP can provide the services they propose.

NEW QUESTION 398

- (Topic 3)

Which of the following is the BEST information source for management to use as an aid in the identification of assets that are subject to laws and regulations?

- A. Security incident summaries

- B. Vendor best practices
- C. CERT coordination center
- D. Significant contracts

Answer: D

Explanation:

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

NEW QUESTION 401

- (Topic 3)

Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

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

Answer: B

Explanation:

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

NEW QUESTION 406

- (Topic 3)

The risks associated with electronic evidence gathering would MOST likely be reduced by an e-mail:

- A. destruction policy
- B. security policy
- C. archive policy
- D. audit policy

Answer: C

Explanation:

With a policy of well-archived e-mail records, access to or retrieval of specific e-mail records is possible without disclosing other confidential e-mail records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying e-mails may be an illegal act.

NEW QUESTION 409

- (Topic 3)

The output of the risk management process is an input for making:

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

Answer: C

Explanation:

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

NEW QUESTION 413

- (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 415

- (Topic 3)

A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:

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

Answer: C

Explanation:

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

NEW QUESTION 420

- (Topic 3)

Which of the following does a lack of adequate security controls represent?

- A. Threat
- B. Asset
- C. Impact
- D. Vulnerability

Answer: D

Explanation:

The lack of adequate security controls represents a vulnerability, exposing sensitive information and data to the risk of malicious damage, attack or unauthorized access by hackers. This could result in a loss of sensitive information and lead to the loss of goodwill for the organization. A succinct definition of risk is provided by the Guidelines for the Management of IT Security published by the International Organization for Standardization (ISO), which defines risk as the 'potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.' The various elements of the definition are vulnerability, threat, asset and impact. Lack of adequate security functionality in this context is a vulnerability.

NEW QUESTION 425

- (Topic 3)

Assessing IT risks is BEST achieved by:

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

Answer: A

Explanation:

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

NEW QUESTION 430

- (Topic 3)

Which of the following should be the MOST important consideration when deciding areas of priority for IT governance implementation?

- A. Process maturity
- B. Performance indicators
- C. Business risk
- D. Assurance reports

Answer: C

Explanation:

Priority should be given to those areas which represent a known risk to the enterprise's operations. The level of process maturity, process performance and audit reports will feed into the decision making process. Those areas that represent real risk to the business should be given priority.

NEW QUESTION 433

- (Topic 3)

During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described IT risks. What is the MOST appropriate recommendation in this situation?

- A. Create an IT risk management department and establish an IT risk framework with the aid of external risk management expert
- B. Use common industry standard aids to divide the existing risk documentation into several individual risks which will be easier to handle
- C. No recommendation is necessary since the current approach is appropriate for a medium-sized organization
- D. Establish regular IT risk management meetings to identify and assess risks, and create a mitigation plan as input to the organization's risk management

Answer: D**Explanation:**

Establishing regular meetings is the best way to identify and assess risks in a medium-sized organization, to address responsibilities to the respective management and to keep the risk list and mitigation plans up to date. A medium-sized organization would normally not have a separate IT risk management department. Moreover, the risks are usually manageable enough so that external help would not be needed. While common risks may be covered by common industry standards, they cannot address the specific situation of an organization. Individual risks will not be discovered without a detailed assessment from within the organization. Splitting the one risk position into several is not sufficient.

NEW QUESTION 437

- (Topic 3)

The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

- A. financial result
- B. customer satisfaction
- C. internal process efficiency
- D. innovation capacity

Answer: A**Explanation:**

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

NEW QUESTION 438

- (Topic 3)

Before implementing an IT balanced scorecard, an organization must:

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

Answer: B**Explanation:**

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

NEW QUESTION 441

- (Topic 4)

The most common reason for the failure of information systems to meet the needs of users is that:

- A. user needs are constantly changing
- B. the growth of user requirements was forecast inaccurately
- C. the hardware system limits the number of concurrent users
- D. user participation in defining the system's requirements was inadequate

Answer: D**Explanation:**

Lack of adequate user involvement, especially in the system's requirements phase, will usually result in a system that does not fully or adequately address the needs of the user. Only users can define what their needs are, and therefore what the system should accomplish.

NEW QUESTION 444

- (Topic 4)

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

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

Answer:

C

Explanation:

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

NEW QUESTION 445

- (Topic 4)

Which of the following should an IS auditor review to gain an understanding of the effectiveness of controls over the management of multiple projects?

- A. Project database
- B. Policy documents
- C. Project portfolio database
- D. Program organization

Answer: C**Explanation:**

A project portfolio database is the basis for project portfolio management. It includes project data, such as owner, schedules, objectives, project type, status and cost. Project portfolio management requires specific project portfolio reports. A project database may contain the above for one specific project and updates to various parameters pertaining to the current status of that single project. Policy documents on project management set direction for the design, development, implementation and monitoring of the project. Program organization is the team required (steering committee, quality assurance, systems personnel, analyst, programmer, hardware support, etc.) to meet the delivery objective of the project.

NEW QUESTION 447

- (Topic 4)

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

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

Answer: B**Explanation:**

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

NEW QUESTION 451

- (Topic 4)

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

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

Answer: D**Explanation:**

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

NEW QUESTION 454

- (Topic 4)

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

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

Answer: C**Explanation:**

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

NEW QUESTION 456

- (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. integrity
- B. authenticity
- C. authorization
- D. nonrepudiation

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 459

- (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 461

- (Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 463

- (Topic 4)

To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

- A. during data preparation
- B. in transit to the computer
- C. between related computer runs
- D. during the return of the data to the user department

Answer: A

Explanation:

During data preparation is the best answer, because it establishes control at the earliest point.

NEW QUESTION 465

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 469

- (Topic 4)

The MAIN purpose of a transaction audit trail is to:

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

Answer: B

Explanation:

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

NEW QUESTION 472

- (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 improvement
- B. quantitative quality goal
- C. a documented process
- 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 474

- (Topic 4)

Which of the following is the most important element in the design of a data warehouse?

- A. Quality of the metadata
- B. Speed of the transactions
- C. Volatility of the data
- D. Vulnerability of the system

Answer: A

Explanation:

Quality of the metadata is the most important element in the design of a data warehouse. A data warehouse is a copy of transaction data specifically structured for query and analysis. Metadata aim to provide a table of contents to the information stored in the data warehouse. Companies that have built warehouses believe that metadata are the most important component of the warehouse.

NEW QUESTION 477

- (Topic 4)

Ideally, stress testing should be carried out in a:

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

Answer: C

Explanation:

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

NEW QUESTION 480

- (Topic 4)

Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?

- A. inheritance
- B. Dynamic warehousing
- C. Encapsulation
- D. Polymorphism

Answer: C

Explanation:

Encapsulation is a property of objects, and it prevents accessing either properties or methods that have not been previously defined as public. This means that any implementation of the behavior of an object is not accessible. An object defines a communication interface with the exterior and only that which belongs to that interface can be accessed.

NEW QUESTION 483

- (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 484

- (Topic 4)

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

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

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 487

- (Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 492

- (Topic 4)

The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:

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

Answer: B

Explanation:

Decision trees use questionnaires to lead a user through a series of choices until a conclusion is reached. Rules refer to the expression of declarative knowledge through the use of if-then relationships. Semantic nets consist of a graph in which nodes represent physical or conceptual objects and the arcs describe the

relationship between the nodes. Semantic nets resemble a dataflow diagram and make use of an inheritance mechanism to prevent duplication of data.

NEW QUESTION 494

- (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 496

- (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 498

- (Topic 4)

The GREATEST advantage of rapid application development (RAD) over the traditional system development life cycle (SDLC) is that it:

- A. facilitates user involvement
- B. allows early testing of technical features
- C. facilitates conversion to the new system
- D. shortens the development time frame

Answer: D

Explanation:

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

NEW QUESTION 499

- (Topic 4)

An IS auditor reviewing a proposed application software acquisition should ensure that the:

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

Answer: D

Explanation:

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

NEW QUESTION 503

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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