Exam A

QUESTION 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

Correct Answer: D

Explanation: 4GLs are usually not suitable for data-intensive operations. They are mainly used for graphic user interface (GUI) design or as simple query/report generators.

QUESTION 2

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

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

Correct Answer: D

Explanation: A before-and-after maintenance report is the best method, as it provides the most positive verification that the updates were executed correctly.

QUESTION 3

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

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

Correct Answer: A

Explanation: A blackbox test is a dynamic analysis tool that tests software modules by examining the behavior of the software without knowledge of its internal workings.

QUESTION 4

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) Weaker organizational structures and less accountability
D) Increased information protection (IP) risk will increase

Correct Answer: A

Explanation: A BPR project often leads to an increased number of people using technology, which can raise concerns about technology adoption and its implications.

QUESTION 5

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

A) Router
B) Bridge
C) Repeater
D) Gateway

Correct Answer: B

Explanation: A bridge connects two separate networks to form a logical network and has the capability to store frames and act as a storage-and-forward device.

QUESTION 6

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

A) Provide an audit trail

B) Can be used in a switchboard environment

C) Permit unlimited user mobility

D) Allow call forwarding

Correct Answer: A

Explanation: A callback feature logs all authorized and unauthorized access attempts, allowing for follow-up and review of potential breaches.

QUESTION 7

A call-back system requires that a user with an ID and password call a remote server through a dial-up line. The server then 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.

Correct Answer: A

Explanation: A call-back system dials back to the user machine using a stored telephone number from its database after initial connection.

QUESTION 8

Structured programming is BEST described as a technique that:

A) Provides knowledge of program functions to other programmers via peer reviews.

B) Reduces the maintenance time of programs by the use of small-scale program modules.

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 process.

Correct Answer: B

Explanation: Structured programming emphasizes small, manageable modules, which are easier to maintain and debug.

QUESTION 9

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

Correct Answer: B

Explanation: A check digit is a numeric value appended to data, calculated mathematically, and helps detect errors such as transposition or transcription.

QUESTION 10

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

A) Cold site.

B) Warm site.

C) Dial-up site.
D) Duplicate processing facility.
Correct Answer: A
Explanation: A cold site is prepared to receive equipment but does not have any components installed ahead of need.

QUESTION 11
Question: A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

- **Unit testing**
- **Integration testing** (Correct Answer)
- **Design walk-throughs**
- **Configuration management**

Explanation:
A common issue in system maintenance is that quick corrections lead to insufficient testing, particularly in integration testing. Integration testing ensures that all components of a system work together correctly, and failures during acceptance testing suggest this phase was not adequately performed.

QUESTION 12
Question: In an EDI process, the device which transmits and receives electronic documents is the:

- **communications handler.** (Correct Answer)
- **EDI translator.**
- **application interface.**
- **EDI interface.**

Explanation:
The communications handler is responsible for transmitting and receiving electronic documents between trading partners and networks, making it a crucial component in the EDI process.

QUESTION 13
Question: The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

- **testing stage.**
- **evaluation stage.**
- **maintenance stage.**
- **early stages of planning.** (Correct Answer)

Explanation:
The most effort in BCP typically occurs during the early stages of planning, where the framework and resources are established. This sets the foundation for the subsequent phases of maintenance, testing, and evaluation.

QUESTION 14
Question: Which of the following network configuration options contains a direct link between any two host machines?

- **Bus**
- **Ring**
- **Star**
- **Completely connected (mesh)** (Correct Answer)

Explanation:
A completely connected (mesh) configuration allows for a direct link between any two host machines, ensuring redundancy and reliability in network communications.

QUESTION 15
Question: Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

- **Check digit**
- **Existence check**
- **Completeness check** (Correct Answer)
- **Reasonableness check**

Explanation:
A completeness check verifies that a field contains actual data, excluding blanks or zeros, ensuring that all necessary information is present.

QUESTION 16
Question: Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

- **A substantive test of program library controls**
- **A compliance test of program library controls** (Correct Answer)
- **A compliance test of the program compiler controls**
- **A substantive test of the program compiler controls**

Explanation:
A compliance test checks whether controls are operating as designed. In this case, the auditor is verifying if the source and object code versions match as per the established controls in the program library.

QUESTION 17
Question: A data administrator is responsible for:

- **maintaining database system software.**
- **defining data elements, data names and their relationship.** (Correct Answer)
- **developing physical database structures.**
- **developing data dictionary system software.**

Explanation:
The primary role of a data administrator includes defining data elements, names, and their relationships, while tasks such as maintaining database software are typically the responsibility of a database administrator (DBA).

QUESTION 18
Question: A database administrator is responsible for:

- **defining data ownership.**
- **establishing operational standards for the data dictionary.**
- **creating the logical and physical database.** (Correct Answer)
- **establishing ground rules for ensuring data integrity and security.**

Explanation:
The DBA's key responsibility is to create and manage the logical and physical structure of the database. Data ownership is usually defined by user departments, while operational standards and security rules are typically collaborative efforts.

QUESTION 19
Question: An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

- **defining the conceptual schema.**
- **defining security and integrity checks.**
- **liaising with users in developing data model.**
- **mapping data model with the internal schema.** (Correct Answer)

Explanation:
Mapping the data model to the internal schema is rarely the responsibility of a DBA, as this could compromise data

independence. This task is typically handled during the conceptual schema phase, which precedes the physical implementation.

QUESTION 20

Question: To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:

- **the entire message and thereafter enciphering the message digest using the sender's private key.** (Correct Answer)
- **any arbitrary part of the message and thereafter enciphering the message digest using the sender's private key.**
- **the entire message and thereafter enciphering the message using the sender's private key.**
- **the entire message and thereafter enciphering the message along with the message digest using the sender's private key.**

Explanation:

To create a digital signature, the sender first generates a message digest of the entire message, which is then encrypted using the sender's private key, ensuring data integrity and authenticity.

QUESTION 21

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

- **digest signature.**
- **electronic signature.**
- **digital signature.** (Correct Answer)
- **hash signature.**

Explanation:

A digital signature is created using a cryptographic algorithm to provide authenticity and integrity to a digital document. It ensures that the message comes from the stated sender and has not been altered.

QUESTION 22

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

- **special router that connects the Internet to a LAN.**
- **device for preventing authorized users from accessing the LAN.** (Correct Answer)
- **server used to connect authorized users to private trusted network resources.**
- **proxy server to increase the speed of access to authorized users.**

Explanation:

Firewalls are designed to protect private networks from unauthorized access, filtering incoming and outgoing traffic based on predefined security rules.

QUESTION 23

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

- **Spool**
- **Cluster controller**
- **Protocol converter**
- **Front end processor** (Correct Answer)

Explanation:

A front-end processor manages communications and relieves the central computer from the burden of handling message formatting and control, enhancing overall network efficiency.

QUESTION 24

Question: The use of a GANTT chart can:

- **aid in scheduling project tasks.** (Correct Answer)
- **determine project checkpoints.**
- **ensure documentation standards.**
- **direct the post-implementation review.**

Explanation:
A GANTT chart is primarily used for scheduling tasks in a project, visually representing timelines and progress.

QUESTION 25
Question: Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

- **Gateway** (Correct Answer)
- **Protocol converter**
- **Front-end communication processor**
- **Concentrator/multiplexor**

Explanation:
A gateway connects different networks and translates data formats, allowing messages to be transmitted between diverse network architectures.

QUESTION 26
Question: Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

- **Specific developments only**
- **Business requirements only**
- **All phases of the installation must be documented** (Correct Answer)
- **No need to develop a customer-specific documentation**

Explanation:
Comprehensive documentation covering all phases of the EPR software installation is essential to ensure quality, understanding, and compliance with standards.

QUESTION 27
Question: A hub is a device that connects:

- **two LANs using different protocols.**
- **a LAN with a WAN.**
- **a LAN with a metropolitan area network (MAN).**
- **two segments of a single LAN.** (Correct Answer)

Explanation:
A hub operates at the physical layer and connects multiple segments of the same LAN, effectively acting as a simple repeater for network signals.

QUESTION 28
Question: A LAN administrator normally would be restricted from:

- **having end-user responsibilities.**
- **reporting to the end-user manager.**
- **having programming responsibilities.** (Correct Answer)
- **being responsible for LAN security administration.**

Explanation:
A LAN administrator typically focuses on network management and support, while programming tasks are usually assigned to developers or programmers.

QUESTION 29
Question: Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?

- **Multiplexer**
- **Modem** (Correct Answer)
- **Protocol converter**
- **Concentrator**

Explanation:
A modem (modulator-demodulator) converts digital signals to analog for transmission over telephone lines and vice versa.

QUESTION 30
Question: Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

- **A neural network** (Correct Answer)
- **Database management software**
- **Management information systems**
- **Computer assisted audit techniques**

Explanation:
Neural networks are capable of learning and identifying patterns in data, making them effective for monitoring and reporting anomalies in financial transactions.

Feel free to ask if you have any further questions or need more information!

QUESTION 31
Question: A hardware control that helps to detect errors when data are communicated from one computer to another is known as a:

- **duplicate check.**
- **table lookup.**
- **validity check.**
- **parity check.** (Correct Answer)

Explanation:
A parity check adds an extra bit (the parity bit) to a data item to indicate whether the total number of 1-bits is odd or even, helping to detect errors in data transmission.

QUESTION 32
Question: For which of the following applications would rapid recovery be MOST crucial?

- **Point-of-sale system** (Correct Answer)
- **Corporate planning**
- **Regulatory reporting**
- **Departmental chargeback**

Explanation:
A point-of-sale system is critical for real-time transactions and inventory management. Downtime can directly affect revenue generation and operational efficiency.

QUESTION 33
Question: The initial step in establishing an information security program is the:

- **development and implementation of an information security standards manual.**
- **performance of a comprehensive security control review by the IS auditor.**
- **adoption of a corporate information security policy statement.** (Correct Answer)
- **purchase of security access control software.**

Explanation:
The adoption of a corporate information security policy statement provides a framework and demonstrates management’s commitment to security, laying the groundwork for the entire security program.

QUESTION 34

Question: A malicious code that changes itself with each file it infects is called a:

- **logic bomb.**
- **stealth virus.**
- **trojan horse.**
- **polymorphic virus.** (Correct Answer)

Explanation:

A polymorphic virus can modify its code with each infection, making it difficult for antivirus software to detect it consistently due to the lack of a fixed pattern.

QUESTION 35

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

- **Paper test**
- **Post test**
- **Preparedness test** (Correct Answer)
- **Walk-through**

Explanation:

A preparedness test is a scaled-back version of a full test, using real resources to simulate a disaster scenario, helping to evaluate the effectiveness of the continuity plan.

QUESTION 36

Question: An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST cost-effective test of the DRP?

- **Full operational test**
- **Preparedness test** (Correct Answer)
- **Paper test**
- **Regression test**

Explanation:

A preparedness test evaluates the readiness of each location's operations for disaster recovery, making it a practical and cost-effective approach for geographically dispersed offices.

QUESTION 37

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

- **Relocate the shut-off switch.**
- **Install protective covers.** (Correct Answer)
- **Escort visitors.**
- **Log environmental failures.**

Explanation:

Installing protective covers over critical switches can prevent accidental activation while still allowing access when needed, enhancing operational safety.

QUESTION 38

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

- **Acceptance testing is to be managed by users.**
- **A quality plan is not part of the contracted deliverables.** (Correct Answer)
- **Not all business functions will be available on initial implementation.**

- **Prototyping is being used to confirm that the system meets business requirements.**

Explanation:
A comprehensive quality plan is essential to ensure the development process meets standards and that all phases of the project are thoroughly managed. Lack of this can lead to significant issues in the final product.

QUESTION 39
Question: In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

- **registration authority (RA).** (Correct Answer)
- **issuing certification authority (CA).**
- **subject CA.**
- **policy management authority.**

Explanation:
The RA is responsible for verifying the identity of certificate applicants before issuing digital certificates, ensuring that only authorized individuals obtain them.

QUESTION 40
Question: Which of the following is a data validation edit and control?

- **Hash totals**
- **Reasonableness checks** (Correct Answer)
- **Online access controls**
- **Before and after image reporting**

Explanation:
Reasonableness checks are used to validate data by ensuring that it meets predetermined criteria, helping to identify anomalies and maintain data integrity.

QUESTION 41
Question: A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

- **reasonableness check.**
- **parity check.**
- **redundancy check.** (Correct Answer)
- **check digits.**

Explanation:
A redundancy check helps detect transmission errors by adding calculated bits to the end of data segments, ensuring that the data received matches what was sent.

QUESTION 42
Question: What is the primary objective of a control self-assessment (CSA) program?

- **Enhancement of the audit responsibility.** (Correct Answer)
- **Elimination of the audit responsibility.**
- **Replacement of the audit responsibility.**
- **Integrity of the audit responsibility.**

Explanation:
The primary goal of a CSA program is to enhance audit responsibilities by involving management and staff in assessing the effectiveness of controls.

QUESTION 43
Question: IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

- **True.** (Correct Answer)

- **False.**

Explanation:
If IS auditors find that control risks are within acceptable limits, they are more likely to perform compliance tests to validate reliance on those internal controls.

QUESTION 44
Question: As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

- **The same value.**
- **Greater value.**
- **Lesser value.** (Correct Answer)
- **Prior audit reports are not relevant.**

Explanation:
Prior audit reports are generally considered of lesser value because they may not reflect the current state of controls or processes compared to direct evidence collected during an audit.

QUESTION 45
Question: What is the PRIMARY purpose of audit trails?

- **To document auditing efforts.**
- **To correct data integrity errors.**
- **To establish accountability and responsibility for processed transactions.** (Correct Answer)
- **To prevent unauthorized access to data.**

Explanation:
Audit trails are primarily used to establish accountability by tracking who processed transactions and when, thereby supporting transparency and traceability.

QUESTION 46
Question: How does the process of systems auditing benefit from using a risk-based approach to audit planning?

- **Controls testing starts earlier.**
- **Auditing resources are allocated to the areas of highest concern.** (Correct Answer)
- **Auditing risk is reduced.**
- **Controls testing is more thorough.**

Explanation:
A risk-based approach ensures that auditing resources focus on the highest risk areas, optimizing the effectiveness of the audit process.

QUESTION 47
Question: After an IS auditor has identified threats and potential impacts, the auditor should:

- **Identify and evaluate the existing controls.** (Correct Answer)
- **Conduct a business impact analysis (BIA).**
- **Report on existing controls.**
- **Propose new controls.**

Explanation:
The next logical step after identifying threats is to assess the existing controls to determine their adequacy in mitigating those threats.

QUESTION 48
Question: The use of statistical sampling procedures helps minimize:

- **Detection risk.** (Correct Answer)
- **Business risk.**
- **Controls risk.**
- **Compliance risk.**

Explanation:
Statistical sampling reduces detection risk by allowing auditors to make inferences about the population based on a representative sample, increasing the reliability of the audit results.

QUESTION 49
Question: What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

- **Business risk.**
- **Detection risk.** (Correct Answer)
- **Residual risk.**
- **Inherent risk.**

Explanation:
Detection risk occurs when an auditor fails to detect material misstatements due to ineffective testing, leading to incorrect conclusions about the accuracy of the financial information.

QUESTION 50
Question: A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:

- **Identify high-risk areas that might need a detailed review later.** (Correct Answer)
- **Reduce audit costs.**
- **Reduce audit time.**
- **Increase audit accuracy.**

Explanation:
CSA techniques help organizations identify areas of high risk, allowing for targeted audits and more efficient allocation of audit resources.

QUESTION 51
Question: What type of approach to the development of organizational policies is often driven by risk assessment?

- **Bottom-up**
- **Top-down** (Correct Answer)
- **Comprehensive**
- **Integrated**

Explanation:
A top-down approach is typically driven by risk assessments, ensuring that policies align with organizational goals and address identified risks.

QUESTION 52
Question: Who is accountable for maintaining appropriate security measures over information assets?

- **Data and systems owners.** (Correct Answer)
- **Data and systems users.**
- **Data and systems custodians.**
- **Data and systems auditors.**

Explanation:
Data and systems owners are ultimately responsible for ensuring that adequate security measures are implemented and maintained for their information assets.

QUESTION 53
Question: Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

- **True.** (Correct Answer)
- **False.**

Explanation:
Proper segregation of duties is essential to prevent conflicts of interest and ensure that no single individual has control over multiple related tasks, such as system development and quality assurance.

QUESTION 54
Question: What should an IS auditor do if he or she observes that project-approval procedures do not exist?

- **Advise senior management to invest in project-management training for the staff.**
- **Create project-approval procedures for future project implementations.**
- **Assign project leaders.**
- **Recommend to management that formal approval procedures be adopted and documented.** (Correct Answer)

Explanation:
The IS auditor should recommend the establishment and documentation of formal project-approval procedures to ensure consistency and oversight in project management.

QUESTION 55
Question: Who is ultimately accountable for the development of an IS security policy?

- **The board of directors.** (Correct Answer)
- **Middle management.**
- **Security administrators.**
- **Network administrators.**

Explanation:
The board of directors has ultimate accountability for the development and approval of IS security policies, reflecting the organization's commitment to security.

QUESTION 56
Question: Proper segregation of duties normally does not prohibit a LAN administrator from also having programming responsibilities. True or false?

- **True.**
- **False.** (Correct Answer)

Explanation:
Proper segregation of duties generally prohibits a LAN administrator from also having programming responsibilities to mitigate risks associated with conflicts of interest and fraud.

QUESTION 57
Question: A core tenant of an IS strategy is that it must:

- **Be inexpensive.**
- **Be protected as sensitive confidential information.**
- **Protect information confidentiality, integrity, and availability.**
- **Support the business objectives of the organization.** (Correct Answer)

Explanation:
An effective IS strategy must align with and support the overall business objectives of the organization, ensuring that IT initiatives contribute to strategic goals.

QUESTION 58
Question: Batch control reconciliation is a ______________________ (fill in the blank) control for mitigating risk of inadequate segregation of duties.

- **Detective**
- **Corrective**
- **Preventative**
- **Compensatory.** (Correct Answer)

Explanation:
Batch control reconciliation serves as a compensatory control, helping to mitigate risks arising from inadequate segregation of duties by ensuring that processed transactions are accurately recorded and verified.

QUESTION 59
Question: Key verification is one of the best controls for ensuring that:

- **Data is entered correctly.** (Correct Answer)
- **Only authorized cryptographic keys are used.**
- **Input is authorized.**
- **Database indexing is performed properly.**

Explanation:
Key verification processes help ensure the accuracy of data entry by validating that the correct information is inputted into systems.

QUESTION 60
Question: If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

- **IT cannot be implemented if senior management is not committed to strategic planning.**
- **More likely.**
- **Less likely.** (Correct Answer)
- **Strategic planning does not affect the success of a company's implementation of IT.**

Explanation:
The lack of commitment from senior management to strategic planning makes successful IT implementation less likely, as strategic alignment and support are crucial for achieving organizational goals.

Question 61
Which of the following could lead to an unintentional loss of confidentiality? Choose the BEST answer.

- A. Lack of employee awareness of a company's information security policy
- B. Failure to comply with a company's information security policy
- C. A momentary lapse of reason
- D. Lack of security policy enforcement procedures

Correct Answer: A
Explanation: Lack of employee awareness of a company's information security policy could lead to an unintentional loss of confidentiality.

Question 62
What topology provides the greatest redundancy of routes and the greatest network fault tolerance?

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

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

Question 63
An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

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

- D. Evidence collected through transaction reports provided by the organization's IT administration

Correct Answer: A

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

Question 64

What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?

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

Correct Answer: B

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

Question 65

How is the time required for transaction processing review usually affected by properly implemented Electronic Data Interface (EDI)?

- A. EDI usually decreases the time necessary for review.
- B. EDI usually increases the time necessary for review.
- C. Cannot be determined.
- D. EDI does not affect the time necessary for review.

Correct Answer: A

Explanation: Electronic Data Interface (EDI) supports inter-vendor communication while decreasing the time necessary for review because it is usually configured to readily identify errors requiring follow-up.

Question 66

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

Correct Answer: B

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

Question 67

Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirety or not at all. Atomicity is part of the ACID test reference for transaction processing. True or false?

- A. True
- B. False

Correct Answer: A

Explanation: Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirety or not at all. Atomicity is part of the ACID test reference for transaction processing.

Question 68

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

Correct 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.

Question 69
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

Correct 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.

Question 70
How is risk affected if users have direct access to a database at the system level?

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

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

Question 71
What is the most common purpose of a virtual private network implementation?

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

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

Question 72
What benefit does using capacity-monitoring software to monitor usage patterns and trends provide to management? Choose the BEST answer.

- A. The software can dynamically readjust network traffic capabilities based upon current usage.
- B. The software produces nice reports that really impress management.
- C. It allows users to properly allocate resources and ensure continuous efficiency of operations.
- D. It allows management to properly allocate resources and ensure continuous efficiency of operations.

Correct Answer: D
Explanation: Using capacity-monitoring software to monitor usage patterns and trends enables management to properly allocate resources and ensure continuous efficiency of operations.

Question 73
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

Correct Answer: B

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

Question 74

What are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information? Choose the BEST answer.

- A. Referential integrity controls
- B. Normalization controls
- C. Concurrency controls
- D. Run-to-run totals

Correct Answer: C

Explanation: Concurrency controls are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information.

Question 75

What increases encryption overhead and cost the most?

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

Correct Answer: B

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

Question 76

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

Correct Answer: A

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

Question 77

What is an initial step in creating a proper firewall policy?

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

Correct Answer: C

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

Question 78

What type of cryptosystem is characterized by data being encrypted by the sender using the recipient's public key, and the data then being decrypted using the recipient's private key?

- A. With public-key encryption, or symmetric encryption
- B. With public-key encryption, or asymmetric encryption
- C. With shared-key encryption, or symmetric encryption
- D. With shared-key encryption, or asymmetric encryption

Correct Answer: B

Explanation: With public-key encryption or asymmetric encryption, data is encrypted by the sender using the recipient's public key; the data is then decrypted using the recipient's private key.

Question 79

How does the SSL network protocol provide confidentiality?

- A. Through symmetric encryption such as RSA
- B. Through asymmetric encryption such as Data Encryption Standard, or DES
- C. Through asymmetric encryption such as Advanced Encryption Standard, or AES
- D. Through symmetric encryption such as Data Encryption Standard, or DES

Correct Answer: D

Explanation: The SSL network protocol provides confidentiality through symmetric encryption, primarily using the Data Encryption Standard (DES).

Question 80

What are used as the framework for developing logical access controls?

- A. Information systems security policies
- B. Organizational security policies
- C. Access Control Lists (ACL)
- D. Organizational charts for identifying roles and responsibilities

Correct Answer: A

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

Question 81

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

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

Correct Answer: C

Explanation: Time stamps are an effective control for detecting duplicate transactions, such as payments made or received, by providing a record of when transactions occur.

Question 82

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

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

Correct Answer: C

Explanation: File encryption is a strong control for protecting confidential data on a PC, ensuring that data is unreadable without the proper decryption key.

Question 83

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

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

Correct Answer: B

Explanation: A guiding best practice is to grant access on a least-privilege basis according to the organization's data owners, minimizing exposure to sensitive data.

Question 84

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

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

Correct Answer: C

Explanation: Public Key Infrastructure (PKI) combines public-key cryptography and digital certificates to enhance confidentiality, reliability, and integrity of Internet transactions.

Question 85

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

Correct Answer: A

Explanation: Digital signatures primarily provide authentication and integrity of data, ensuring that the data comes from a verified source and has not been altered.

Question 86

Regarding digital signature implementation, which of the following answers is correct?

- A. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's private key. Upon receiving the data, the recipient can decrypt the data using the sender's public key.
- B. A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's public key.
- C. A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value or message digest from the entire message contents. Upon receiving the data, the recipient can independently create it.
- D. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's private key.

Correct Answer: C

Explanation: A digital signature involves creating a hash value of the message contents for integrity validation. The recipient can then independently verify the integrity by comparing hash values.

Question 87

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

Correct Answer: D

Explanation: A fingerprint scanner provides a very high degree of access control because biometric systems are difficult to forge and provide strong authentication.

Question 88

What are often the primary safeguards for systems software and data?

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

Correct Answer: B

Explanation: Logical access controls are typically the primary safeguards for systems software and data, determining who has access to what within the system.

Question 89

Which of the following is often used as a detection and deterrent control against Internet attacks?

- A. Honeypots
- B. CCTV
- C. VPN
- D. VLAN

Correct Answer: A

Explanation: Honeypots are designed to attract and trap potential attackers, providing both detection and deterrent capabilities against Internet attacks.

Question 90

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

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

Correct Answer: A

Explanation: A monitored double-doorway entry system, or mantrap, is designed to prevent unauthorized entry by controlling access between two doors.

Question 91

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

Correct Answer: B

Explanation: Application-layer gateways or proxy firewalls are effective for controlling FTP downloads, as they can inspect and filter traffic at the application level.

Question 92

Which of the following provides the strongest authentication for physical access control?

- A. Sign-in logs
- B. Dynamic passwords

- C. Key verification
- D. Biometrics

Correct Answer: D

Explanation: Biometrics provides the strongest authentication method for physical access control because it relies on unique physical traits.

Question 93

What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off? Choose the BEST answer.

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

Correct Answer: C

Explanation: Screensaver passwords are an effective countermeasure to prevent unauthorized access when data entry operators leave their computers unattended.

Question 94

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

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

Correct Answer: C

Explanation: ISPs can implement inbound traffic filtering using Access Control Lists (ACL) to block unauthorized IP packets.

Question 95

What is the key distinction between encryption and hashing algorithms?

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

Correct Answer: B

Explanation: A key distinction is that hashing algorithms are irreversible, meaning you cannot derive the original input from the hash output.

Question 96

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

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

Correct Answer: A

Explanation: Data diddling involves unauthorized changes to data before it is entered into a system, potentially altering the intended information.

Question 97

Which of the following is used to evaluate biometric access controls?

- A. FAR

- B. EER
- C. ERR
- D. FRR

Correct Answer: B
Explanation: The Equal Error Rate (EER) is used to evaluate biometric access controls, indicating the rate at which false acceptances and false rejections occur.

Question 98
Who is ultimately responsible and accountable for reviewing user access to systems?

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

Correct Answer: C
Explanation: Data owners are responsible for reviewing user access to ensure that access privileges align with organizational policies and requirements.

Question 99
Establishing data ownership is an important first step for which of the following processes? Choose the BEST answer.

- A. Assigning user access privileges
- B. Developing organizational security policies
- C. Creating roles and responsibilities
- D. Classifying data

Correct Answer: D
Explanation: Establishing data ownership is crucial for effective data classification, as it helps to identify who is responsible for data handling and protection.

Question 100
Which of the following is MOST critical during the business impact assessment phase of business continuity planning?

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

Correct Answer: A
Explanation: End-user involvement is critical during the business impact assessment phase to ensure that all potential impacts are accurately identified and assessed from the user's perspective.

Question 101
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

Correct Answer: B
Explanation: The preparedness test utilizes actual resources to simulate a system crash and validate the effectiveness of the business continuity plan (BCP).

Question 102

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

Correct Answer: D

Explanation: Disaster recovery for systems specifically aims to make alternative processes and resources available to ensure transaction processing continuity.

Question 103

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

Correct Answer: C

Explanation: A walk-through test requires representatives from each operational area to convene and review the BCP, ensuring all areas are aware of their roles.

Question 104

What influences decisions regarding the 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

Correct Answer: C

Explanation: The criticality of assets is influenced by both the importance of the data and the broader organizational impact of its loss.

Question 105

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

Correct Answer: A

Explanation: A cold site provides essential facilities, such as electricity and HVAC, but lacks the equipment and immediate processing capabilities found in warmer or hot sites.

Question 106

True or False: A disaster recovery plan (DRP) aims to mitigate the risk and impact of major business interruptions, balancing pre-incident operational costs with recovery costs.

- A. True
- B. False

Correct Answer: A

Explanation: The statement is true; DRP aims to reduce recovery time and costs, with pre-incident costs justified by reduced business impact.

Question 107
Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for the recovery of noncritical systems and data?

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

Correct Answer: A
Explanation: A cold site is a suitable option for noncritical systems as it provides basic infrastructure without the immediate need for high availability.

Question 108
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

Correct Answer: B
Explanation: Changes in system assets should be documented within the business continuity plan to maintain an accurate inventory for recovery efforts.

Question 109
Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the _______________. (fill-in-the-blank)

- A. Security administrator
- B. Systems auditor
- C. Board of directors
- D. Financial auditor

Correct Answer: C
Explanation: Executive management, including the board of directors, holds the ultimate responsibility for BCP and DRP plans.

Question 110
True or False: Obtaining user approval of program changes is very effective for controlling application changes and maintenance.

- A. True
- B. False

Correct Answer: A
Explanation: User approval of program changes is an effective measure for maintaining control over application modifications.

Question 111
Library control software restricts source code to:

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

Correct Answer: A
Explanation: Library control software typically restricts source code to read-only access to prevent unauthorized modifications.

Question 112
When is regression testing used to determine whether new application changes have introduced any errors in the remaining unchanged code?

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

Correct Answer: A
Explanation: Regression testing is performed in both program development and change management to ensure that new changes do not negatively affect existing functionality.

Question 113
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

Correct Answer: C
Explanation: Determining time and resource requirements is often the most challenging aspect during the initial stages of application development.

Question 114
What is a primary high-level goal for an auditor who is reviewing a system development project?

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

Correct Answer: C
Explanation: Ensuring that business objectives are met is a fundamental goal for auditors reviewing system development projects.

Question 115
Whenever an application is modified, what should be tested to determine the full impact of the change? Choose the BEST answer.

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

Correct Answer: B
Explanation: The entire program, including interfaces, must be tested to fully understand the impact of any changes.

Question 116
The quality of the metadata produced from a data warehouse is _______________ in the warehouse's design. Choose the BEST answer.

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

Correct Answer: B

Explanation: The quality of metadata is critical in data warehouse design as it directly influences data usability and integrity.

Question 117
True or False: Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs.

- A. True
- B. False

Correct Answer: B
Explanation: FPA estimates size based on inputs, outputs, and files, not just inputs and outputs.

Question 118
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

Correct Answer: A
Explanation: User management is responsible for the ownership of a systems development project and the resulting system.

Question 119
If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

- A. Documentation development
- B. Comprehensive integration testing
- C. Full unit testing
- D. Full regression testing

Correct Answer: B
Explanation: The auditor should recommend comprehensive integration testing to ensure that all modules work correctly together.

Question 120
True or False: 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.

- A. True
- B. False

Correct Answer: B
Explanation: An IS auditor should ensure that adequate and complete documentation exists alongside a focus on system controls during a systems-development project.

QUESTION 121
What is a reliable technique for estimating the scope and cost of a software-development project?

- A. Function point analysis (FPA)
- B. Feature point analysis (FPA)
- C. GANTT
- D. PERT
  Correct Answer: A
  Explanation: A function point analysis (FPA) is a reliable technique for estimating the scope and cost of a software-development project.

QUESTION 122
Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

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

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

QUESTION 123
If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do? Choose the BEST answer.

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

  Correct Answer: C
  Explanation: If an IS auditor observes that an IS department fails to use formal documented methodologies, the auditor should document informal standards, test compliance, and recommend formal policies be developed and implemented.

QUESTION 124
What often results in project scope creep when functional requirements are not defined as well as they could be?

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

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

QUESTION 125
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

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

QUESTION 126
Run-to-run totals can verify data through which stage(s) of application processing?

- A. Initial
- B. Various
- C. Final

- D. Output
  Correct Answer: B
  Explanation: Run-to-run totals can verify data through various stages of application processing.

QUESTION 127
________________ (fill in the blank) is/are ultimately accountable for the functionality, reliability, and security within IT governance. Choose the BEST answer.

- A. Data custodians
- B. The board of directors and executive officers
- C. IT security administration
- D. Business unit managers
  Correct Answer: B
  Explanation: The board of directors and executive officers are ultimately accountable for the functionality, reliability, and security within IT governance.

QUESTION 128
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
  Correct Answer: C
  Explanation: Data-mining techniques can be used to help identify and investigate unauthorized transactions.

QUESTION 129
Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

- A. True
- B. False
  Correct Answer: A
  Explanation: Network environments often add to the complexity of program-to-program communication, making application systems implementation and maintenance more difficult.

QUESTION 130
______________ risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a ______________ risk assessment is more appropriate. Fill in the blanks.

- A. Quantitative; qualitative
- B. Qualitative; quantitative
- C. Residual; subjective
- D. Quantitative; subjective
  Correct Answer: A
  Explanation: Quantitative risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a qualitative risk assessment is more appropriate.

QUESTION 131
What must an IS auditor understand before performing an application audit? Choose the BEST answer.

- A. The potential business impact of application risks.
- B. Application risks must first be identified.
- C. Relative business processes.

- D. Relevant application risks.
  Correct Answer: C
  Explanation: An IS auditor must first understand relative business processes before performing an application audit.

QUESTION 132
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
  Correct Answer: C
  Explanation: Defining the scope of areas to be reviewed is the first step in a business process re-engineering project.

QUESTION 133
When storing data archives off-site, what must be done with the data to ensure data completeness?

- A. The data must be normalized.
- B. The data must be validated.
- C. The data must be parallel-tested.
- D. The data must be synchronized.
  Correct Answer: D
  Explanation: When storing data archives off-site, data must be synchronized to ensure data completeness.

QUESTION 134
Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

- A. Redundancy check
- B. Completeness check
- C. Accuracy check
- D. Parity check
  Correct Answer: A
  Explanation: A redundancy check can help detect transmission errors by appending specially calculated bits onto the end of each segment of data.

QUESTION 135
What is an edit check to determine whether a field contains valid data?

- A. Completeness check
- B. Accuracy check
- C. Redundancy check
- D. Reasonableness check
  Correct Answer: A
  Explanation: A completeness check is an edit check to determine whether a field contains valid data.

QUESTION 136
A transaction journal provides the information necessary for detecting unauthorized _____________ (fill in the blank) from a terminal.

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

- D. Duplication

  Correct Answer: B

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

QUESTION 137

An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

- A. True
- B. False

  Correct Answer: B

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

QUESTION 138

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

  Correct Answer: C

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

QUESTION 139

A check digit is an effective edit check to:

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

  Correct Answer: B

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

QUESTION 140

Parity bits are a control used to validate:

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

  Correct Answer: B

  Explanation: Parity bits are a control used to validate data completeness.

QUESTION 141

The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):

- A. Implementor
- B. Facilitator
- C. Developer
- D. Sponsor

  Correct Answer: B

  Explanation: The traditional role of an IS auditor in a control self-assessment (CSA) is to act as a facilitator, helping the process but not directly implementing or developing it.

QUESTION 142
Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

- A. Proper authentication
- B. Proper identification and authentication
- C. Proper identification
- D. Proper identification, authentication, and authorization

  Correct Answer: B

  Explanation: For accountability to be ensured and nonrepudiation prevented, proper identification and authentication must be performed during access control.

QUESTION 143
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

  Correct Answer: C

  Explanation: Identifying high-risk audit targets is the most critical step in audit planning, as it allows for focusing resources on the areas most likely to have significant issues.

QUESTION 144
To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following? Choose the BEST answer.

- A. The business objectives of the organization
- B. The effect of segregation of duties on internal controls
- C. The point at which controls are exercised as data flows through the system
- D. Organizational control policies

  Correct Answer: C

  Explanation: To evaluate the collective effect of controls, an IS auditor should focus on the point where controls are exercised within the system's data flow.

QUESTION 145
What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

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

  Correct Answer: D

  Explanation: The first step for implementing continuous-monitoring systems is identifying the organization's high-risk areas.

QUESTION 146
What type of risk is associated with authorized program exits (trap doors)? Choose the BEST answer.

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

  Correct Answer: D

  Explanation: Inherent risk is associated with trap doors, which are programmed exits that can potentially be exploited, even if authorized.

QUESTION 147

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

  Correct Answer: B

  Explanation: Generalized audit software is ideal for searching for address field duplications and other data inconsistencies.

QUESTION 148

Which of the following is of greatest concern to the IS auditor?

- A. Failure to report a successful attack on the network
- B. Failure to prevent a successful attack on the network
- C. Failure to recover from a successful attack on the network
- D. Failure to detect a successful attack on the network

  Correct Answer: A

  Explanation: Not reporting a successful attack on the network is the most concerning, as it prevents timely action from being taken.

QUESTION 149

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

  Correct Answer: B

  Explanation: This statement is false. An integrated test facility is useful because it can compare the processing output with independently calculated data.

QUESTION 150

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

- A. True
- B. False

  Correct Answer: A

  Explanation: A continuous audit approach improves system security in environments that process large numbers of transactions by providing real-time monitoring and detection.

QUESTION 151

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

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

  Correct Answer: A

  Explanation: The IS auditor's primary responsibility is to advise senior management on risks like improper segregation of duties.

QUESTION 152

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

  Correct Answer: B

  Explanation: Business unit management is responsible for implementing cost-effective controls in automated systems.

QUESTION 153

Why does an IS auditor review an organization chart?

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

  Correct Answer: C

  Explanation: An IS auditor reviews the organizational chart to understand the responsibilities and authority within the organization.

QUESTION 154

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

  Correct Answer: A

  Explanation: The primary objective of an IT security policies audit is to ensure security and control policies align with business and IT objectives.

QUESTION 155

When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.

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

  Correct Answer: D

  Explanation: When auditing third-party service providers, an auditor should be concerned with the ownership of programs and files, due care and confidentiality statements, and the provider's ability to continue service after a disaster.

QUESTION 156

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

- A. True
- B. False

  Correct Answer: B

  Explanation: When auditing IS strategy, the focus should not only be on procedures but on aligning strategy with organizational objectives and external environment considerations.

QUESTION 157

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

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

  Correct Answer: C

  Explanation: IS assessment methods are used by management to determine whether the organization's activities align with its expected levels.

QUESTION 158

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.

  Correct Answer: A

  Explanation: Reviewing the business plan should come before reviewing the IT strategic plan to ensure that the IT strategy aligns with business objectives.

QUESTION 159

Allowing application programmers to directly patch or change code in production programs increases the risk of fraud. True or false?

- A. True
- B. False

  Correct Answer: A

  Explanation: Allowing programmers to directly patch or change production code increases the risk of fraud due to lack of segregation of duties.

QUESTION 160

Who should be responsible for network security operations?

- A. Business unit managers
- B. Security administrators
- C. Network administrators
- D. IS auditors

  Correct Answer: B

  Explanation: Security administrators are responsible for managing and ensuring the security of network operations.

QUESTION 161

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

Correct Answer: A

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

QUESTION 162

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

Correct 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.

QUESTION 163

The directory system of a database-management system describes:

A. The access method to the data

B. The location of data AND the access method

C. The location of data

D. Neither the location of data NOR the access method

Correct Answer: B

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

QUESTION 164

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

Correct Answer: D

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

QUESTION 165

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

A. The data should be deleted and overwritten with binary 0s

B. The data should be demagnetized

C. The data should be low-level formatted

D. The data should be deleted

Correct Answer: B

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

QUESTION 166

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

A. The potential for unauthorized deletion of report copies

B. The potential for unauthorized modification of report copies

C. The potential for unauthorized printing of report copies

D. The potential for unauthorized editing of report copies

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

QUESTION 167
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 SSL
D. WAP often interfaces critical IT systems
Correct 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.

QUESTION 168
Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?
A. True
B. False
Correct Answer: A
Explanation: Proper segregation of duties prevents a computer operator (user) from performing security administration duties.

QUESTION 169
How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?
A. Modems convert analog transmissions to digital, and digital transmission to analog
B. Modems encapsulate analog transmissions within digital, and digital transmissions within analog
C. Modems convert digital transmissions to analog, and analog transmissions to digital
D. Modems encapsulate digital transmissions within analog, and analog transmissions within digital
Correct Answer: A
Explanation: Modems (modulation/demodulation) convert analog transmissions to digital, and digital transmissions to analog, and are required for analog transmissions to enter a digital network.

QUESTION 170
Which of the following are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem?
A. Expert systems
B. Neural networks
C. Integrated synchronized systems
D. Multitasking applications
Correct Answer: B
Explanation: Neural networks are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem.

QUESTION 171
What supports data transmission through split cable facilities or duplicate cable facilities?
A. Diverse routing
B. Dual routing
C. Alternate routing
D. Redundant routing

Correct Answer: A

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

QUESTION 172

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

Correct 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.

QUESTION 173

Which of the following can degrade network performance? Choose the BEST answer.

A. Superfluous use of redundant load-sharing gateways

B. Increasing traffic collisions due to host congestion by creating new collision domains

C. Inefficient and superfluous use of network devices such as switches

D. Inefficient and superfluous use of network devices such as hubs

Correct Answer: D

Explanation: Inefficient and superfluous use of network devices such as hubs can degrade network performance.

QUESTION 174

Which of the following provide(s) near-immediate recoverability for time-sensitive systems and transaction processing?

A. Automated electronic journaling and parallel processing

B. Data mirroring and parallel processing

C. Data mirroring

D. Parallel processing

Correct Answer: B

Explanation: Data mirroring and parallel processing are both used to provide near-immediate recoverability for time-sensitive systems and transaction processing.

QUESTION 175

What is an effective control for granting temporary access to vendors and external support personnel? Choose the BEST answer.

A. Creating user accounts that automatically expire by a predetermined date

B. Creating permanent guest accounts for temporary use

C. Creating user accounts that restrict logon access to certain hours of the day

D. Creating a single shared vendor administrator account on the basis of least-privileged access

Correct Answer: A

Explanation: Creating user accounts that automatically expire by a predetermined date is an effective control for granting temporary access to vendors and external support personnel.

QUESTION 176

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

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

QUESTION 177
What is a common vulnerability, allowing denial-of-service attacks?
A. Assigning access to users according to the principle of least privilege
B. Lack of employee awareness of organizational security policies
C. Improperly configured routers and router access lists
D. Configuring firewall access rules
Correct Answer: C
Explanation: Improperly configured routers and router access lists are a common vulnerability for denial-of-service attacks.

QUESTION 178
What are trojan horse programs? Choose the BEST answer.
A. A common form of internal attack
B. Malicious programs that require the aid of a carrier program such as email
C. Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
D. A common form of Internet attack
Correct Answer: D
Explanation: Trojan horse programs are a common form of Internet attack.

QUESTION 179
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
Correct Answer: A
Explanation: Network performance-monitoring tools are used to measure and ensure proper network capacity management and availability of services.

QUESTION 180
What can be used to gather evidence of network attacks?
A. Access control lists (ACL)
B. Intrusion-detection systems (IDS)
C. Syslog reporting
D. Antivirus programs
Correct Answer: B
Explanation: Intrusion-detection systems (IDS) are used to gather evidence of network attacks.

QUESTION 181
Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?
A. Traffic analysis
B. SYN flood
C. Denial of service (DoS)
D. Distributed denial of service (DDoS)

Correct Answer: A

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

QUESTION 182

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

Correct Answer: C

Explanation: Dry-pipe sprinklers are considered to be the most environmentally friendly fire-suppression method.

QUESTION 183

What is a callback system?

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

Correct Answer: C

Explanation: A callback system is a remote-access control whereby the user initially connects via dial-up, and the server calls the user back at a predetermined number stored in the server's configuration.

QUESTION 184

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

Correct Answer: A

Explanation: A dry-pipe sprinkler system suppresses fire via water delivered through dry pipes installed throughout the facilities.

QUESTION 185

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

Correct Answer: A

Explanation: Digital signatures require the sender to "sign" the data by encrypting it with the sender's private key, and the recipient decrypts it using the sender's public key.

QUESTION 186

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

A. Biometrics
B. Password

C. Token
D. PIN
Correct Answer: A
Explanation: Biometrics provides strong single-factor authentication, as it relies on unique physical attributes of the user.

QUESTION 187
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
Correct Answer: C
Explanation: A website certificate provides authentication of the website and can authenticate keys used for data encryption.

QUESTION 188
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
Correct Answer: B
Explanation: The strength of a secret key in a symmetric cryptosystem is determined by a combination of key length, initial input vectors, and the complexity of the encryption algorithm.

QUESTION 189
What process is used to validate a subject's identity?
A. Identification
B. Nonrepudiation
C. Authorization
D. Authentication
Correct Answer: D
Explanation: Authentication is the process used to validate a subject's identity.

QUESTION 190
What is often assured through table link verification and reference checks?
A. Database integrity
B. Database synchronization
C. Database normalcy
D. Database accuracy
Correct Answer: A
Explanation: Database integrity is ensured through table link verification and reference checks.

QUESTION 191
Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource? Choose the BEST answer.
A. Systems logs
B. Access control lists (ACL)

C. Application logs
D. Error logs
Correct Answer: B
Explanation: Access control lists (ACLs) are reviewed to determine user permissions for a specific resource.

QUESTION 192
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
Correct Answer: B
Explanation: IS auditors should always check to ensure that password files are encrypted.

QUESTION 193
Using the OSI reference model, what layer(s) is/are used to encrypt data?
A. Transport layer
B. Session layer
C. Session and transport layers
D. Data link layer
Correct Answer: C
Explanation: Data encryption is typically performed in the session layer or transport layer of the OSI model.

QUESTION 194
When should systems administrators first assess the impact of applications or systems patches?
A. Within five business days following installation
B. Prior to installation
C. No sooner than five business days following installation
D. Immediately following installation
Correct Answer: B
Explanation: Systems administrators should assess the impact of patches prior to installation.

QUESTION 195
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
Correct Answer: A
Explanation: Adopting and communicating a comprehensive antivirus policy is the most fundamental step in preventing virus attacks.

QUESTION 196
Which of the following is of greatest concern when performing an IS audit?
A. Users' ability to directly modify the database
B. Users' ability to submit queries to the database
C. Users' ability to indirectly modify the database
D. Users' ability to directly view the database
Correct Answer: A
Explanation: A major IS audit concern is users' ability to directly modify the database.

QUESTION 197
What are intrusion-detection systems (IDS) primarily used for?

A. To identify AND prevent intrusion attempts to a network
B. To prevent intrusion attempts to a network
C. Forensic incident response
D. To identify intrusion attempts to a network
Correct Answer: D
Explanation: Intrusion-detection systems (IDS) are primarily used to identify intrusion attempts on a network.

QUESTION 198
Rather than simply reviewing the adequacy of access control, appropriateness of access policies, and effectiveness of safeguards and procedures, the IS auditor is more concerned with effectiveness and utilization of assets. True or false?
A. True
B. False
Correct Answer: B
Explanation: An IS auditor is more concerned with access control, access policies, and effectiveness of safeguards and procedures than with the effectiveness and utilization of assets.

QUESTION 199
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
Correct Answer: A
Explanation: IS auditors are more concerned with a programmer's ability to initiate or modify transactions and access production in live systems than with their ability to authorize transactions.

QUESTION 200
Organizations should use off-site storage facilities to maintain ____________ of current and critical information within backup files. Choose the BEST answer.
A. Confidentiality
B. Integrity
C. Redundancy
D. Concurrency
Correct Answer: C
Explanation: Redundancy is the best answer as it provides both integrity and availability. Organizations should use off-site storage to maintain redundancy of critical information within backup files.

QUESTION 201
The purpose of business continuity planning and disaster-recovery planning is to:

- **A)** Transfer the risk and impact of a business interruption or disaster
- **B)** Mitigate, or reduce, the risk and impact of a business interruption or disaster
- **C)** Accept the risk and impact of a business
- **D)** Eliminate the risk and impact of a business interruption or disaster

Correct Answer: B
Explanation: The primary purpose of business continuity planning (BCP) and disaster recovery planning (DRP) is to mitigate, or reduce, the risk and impact of a business interruption or disaster. Complete elimination of risk is not possible.

QUESTION 202

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

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

Correct Answer: B

Explanation: If a database is restored from information backed up before the last system image, the system should be restarted before the last transaction so that the final transaction can be reprocessed.

QUESTION 203

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

- **A)** True
- **B)** False

Correct Answer: B

Explanation: An off-site processing facility should not be easily identifiable externally as this would make it vulnerable to sabotage or attacks.

QUESTION 204

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

Correct Answer: A

Explanation: Although mitigating the risk and impact of a business interruption is important, the overriding priority in BCP and DRP is always the protection of human life.

QUESTION 205

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

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

Correct Answer: B

Explanation: Geographically dispersing resources reduces the risk of a common disaster affecting all systems, thus mitigating vulnerabilities related to single points of failure.

QUESTION 206

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

- **A)** True
- **B)** False

Correct Answer: A

Explanation: Mitigating the risk and impact of a disaster generally takes priority over transferring risk to an insurer because reducing the risk directly affects the organization's ability to continue operations.

QUESTION 207

Off-site data storage should be kept synchronized when preparing for recovery of time-sensitive data such as that resulting from which of the following?

- **A)** Financial reporting

- **B)** Sales reporting
- **C)** Inventory reporting
- **D)** Transaction processing

Correct Answer: D

Explanation: Time-sensitive data such as transaction processing data must be synchronized with off-site backups to ensure accurate recovery.

QUESTION 208

What is an acceptable recovery mechanism for extremely time-sensitive transaction processing?

- **A)** Off-site remote journaling
- **B)** Electronic vaulting
- **C)** Shadow file processing
- **D)** Storage area network

Correct Answer: C

Explanation: Shadow file processing is an effective recovery mechanism for extremely time-sensitive transaction processing because it allows data to be mirrored and recovered quickly.

QUESTION 209

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

- **A)** Accept
- **B)** Eliminate
- **C)** Transfer
- **D)** Mitigate

Correct Answer: D

Explanation: Off-site backups should be geographically separated to mitigate the risk of widespread disasters such as earthquakes or hurricanes.

QUESTION 210

Why is a clause for requiring source code escrow in an application vendor agreement important?

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

Correct Answer: D

Explanation: A source code escrow ensures that the organization has access to the source code if the vendor goes out of business, allowing them to maintain and modify the application.

QUESTION 211

What uses questionnaires to lead the user through a series of choices to reach a conclusion?

- **A)** Logic trees
- **B)** Decision trees
- **C)** Decision algorithms
- **D)** Logic algorithms

Correct Answer: B

Explanation: Decision trees use a series of questions or choices to guide users to a conclusion, making them useful for decision-making processes.

QUESTION 212

What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

- **A)** Assigning copyright to the organization

- **B)** Program back doors
- **C)** Source code escrow
- **D)** Internal programming expertise

Correct Answer: C

Explanation: Source code escrow protects the organization by ensuring they can access and modify the source code if the vendor goes out of business.

QUESTION 213

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

Correct Answer: A

Explanation: The project sponsor is responsible for ensuring that the requirement specifications are provided to the software development team.

QUESTION 214

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

Correct Answer: D

Explanation: Regression testing should use data from previous tests to ensure accurate conclusions about the effects of program changes or corrections.

QUESTION 215

An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to:

- **A)** Meet business objectives
- **B)** Enforce data security
- **C)** Be culturally feasible
- **D)** Be financially feasible

Correct Answer: A

Explanation: The primary role of an IS auditor is to ensure that the system is designed to meet the business objectives of the project.

QUESTION 216

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

- **A)** Develop test plans.
- **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. The tests verify and validate what has been developed.

Correct Answer: B

Explanation: Procedures to prevent scope creep are established during the design phase of the SDLC to ensure the project stays within its defined boundaries.

QUESTION 217

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

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

Correct Answer: D

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

QUESTION 218

What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality?

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

Correct Answer: A

Explanation: Rapid Application Development (RAD) is a methodology used to develop strategically important systems faster, reduce costs, and maintain quality.

QUESTION 219

Test and development environments should be separated. True or false?

- **A)** True
- **B)** False

Correct Answer: A

Explanation: Test and development environments should be separated to maintain the stability and integrity of testing processes.

QUESTION 220

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

Correct Answer: A

Explanation: Following any changes to an application or system, programmers should perform unit, module, and full regression testing to ensure the changes work as intended and do not introduce new issues.

QUESTION 221

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

- **PERT**
- **Rapid application development (RAD)** (Correct)
- **Function point analysis (FPA)**
- **GANTT**

Explanation:

Rapid Application Development (RAD) focuses on continuous iterations and updating prototypes to meet changing user or business requirements, making it a flexible and adaptive software development method.

QUESTION 222

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

- **Lack of funding**
- **Inadequate user participation during system requirements definition** (Correct)
- **Inadequate senior management participation during system requirements definition**
- **Poor IT strategic planning**

Explanation:

The most common reason for systems failing to meet user needs is inadequate user participation during the requirements definition phase. Users' insights are crucial to defining system functionalities.

QUESTION 223

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

- **The project sponsor**
- **The project steering committee** (Correct)
- **Senior management**
- **The project team leader**

Explanation:

The project steering committee is tasked with overseeing the overall direction, budgets, and schedules of systems-development projects.

QUESTION 224

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

- **In the requirements definition phase of the systems-development project** (Correct)
- **In the feasibility phase of the systems-development project**
- **In the design phase of the systems-development project**
- **In the development phase of the systems-development project**

Explanation:

User acceptance testing (UAT) should be planned early, usually during the requirements definition phase, to ensure the system meets business needs.

QUESTION 225

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

- **Failing to perform user acceptance testing** (Correct)
- **Lack of user training for the new system**
- **Lack of software documentation and run manuals**
- **Insufficient unit, module, and systems testing**

Explanation:

Failing to perform user acceptance testing (UAT) often has the most significant negative impact on the successful implementation of new software, as it ensures that the system meets user needs.

QUESTION 226

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

- **The receiving application**
- **The sending application**
- **Both the sending and receiving applications** (Correct)
- **Output on the sending application and input on the receiving application**

Explanation:

Input/output controls should be implemented on both sending and receiving applications to ensure data accuracy and completeness in an integrated environment.

QUESTION 227

Authentication techniques for sending and receiving data between EDI systems are crucial to prevent which of the following? Choose the BEST answer.

- **Unsynchronized transactions**
- **Unauthorized transactions** (Correct)
- **Inaccurate transactions**
- **Incomplete transactions**

Explanation:

Authentication is essential in Electronic Data Interchange (EDI) systems to prevent unauthorized transactions, ensuring that only approved entities send and receive data.

QUESTION 228

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

- **To evaluate potential countermeasures and compensatory controls**
- **To implement effective countermeasures and compensatory controls**
- **To perform a business impact analysis of the threats that would exploit the vulnerabilities** (Correct)
- **To immediately advise senior management of the findings**

Explanation:

Once vulnerabilities are identified, the IS auditor should conduct a business impact analysis (BIA) to understand the threats and prioritize their mitigation.

QUESTION 229

What is the primary security concern for EDI environments? Choose the BEST answer.

- **Transaction authentication**
- **Transaction completeness**
- **Transaction accuracy**
- **Transaction authorization** (Correct)

Explanation:

In EDI environments, transaction authorization is the primary security concern to ensure that only authorized parties can initiate transactions.

QUESTION 230

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

- **Exposures**
- **Threats** (Correct)
- **Hazards**
- **Insufficient controls**

Explanation:

Threats exploit vulnerabilities, leading to potential loss or damage to the organization’s assets.

QUESTION 231

Business process re-engineering often results in ______________ automation, which results in _____________ number of people using technology. Fill in the blanks.

- **Increased; a greater** (Correct)
- **Increased; a fewer**
- **Less; a fewer**
- **Increased; the same**

Explanation:

Business process re-engineering typically increases automation, which leads to a greater number of people relying on technology in their work processes.

QUESTION 232

Whenever business processes have been re-engineered, the IS auditor attempts to identify and quantify the impact of any controls that might have been removed or controls that might not work as effectively after business process changes. True or false?

- **True** (Correct)
- **False**

Explanation:
It is crucial for the IS auditor to assess the impact on controls when business processes are re-engineered, as this can affect the effectiveness of existing controls or result in their removal.

QUESTION 233
When should an application-level edit check to verify that availability of funds was completed at the electronic funds transfer (EFT) interface?

- **Before transaction completion**
- **Immediately after an EFT is initiated**
- **During run-to-run total testing**
- **Before an EFT is initiated** (Correct)

Explanation:
The availability of funds should be verified before initiating an EFT to ensure the transaction can be completed successfully.

QUESTION 234
________________ (fill in the blank) should be implemented as early as data preparation to support data integrity at the earliest point possible.

- **Control totals** (Correct)
- **Authentication controls**
- **Parity bits**
- **Authorization controls**

Explanation:
Control totals are used to support data integrity by ensuring that data processed matches expected values from the earliest stages of data preparation.

QUESTION 235
What is used as a control to detect loss, corruption, or duplication of data?

- **Redundancy check**
- **Reasonableness check**
- **Hash totals** (Correct)
- **Accuracy check**

Explanation:
Hash totals are used to verify the integrity of data and detect any loss, corruption, or duplication during processing.

QUESTION 236
Data edits are implemented before processing and are considered which of the following? Choose the BEST answer.

- **Deterrent integrity controls**
- **Detective integrity controls**
- **Corrective integrity controls**
- **Preventative integrity controls** (Correct)

Explanation:
Data edits, which are designed to check the accuracy and validity of data before processing, are considered preventive controls.

QUESTION 237
Processing controls ensure that data is accurate and complete, and is processed only through which of the following? Choose the BEST answer.

- **Documented routines**
- **Authorized routines** (Correct)
- **Accepted routines**
- **Approved routines**

Explanation:
Processing controls ensure that data is only processed through authorized routines to maintain accuracy and completeness.

QUESTION 238
What is a data validation edit control that matches input data to an occurrence rate? Choose the BEST answer.

- **Accuracy check**
- **Completeness check**
- **Reasonableness check** (Correct)
- **Redundancy check**

Explanation:
A reasonableness check ensures that the input data is logical and within an expected range based on occurrence rates or other parameters.

QUESTION 239
Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

- **True** (Correct)
- **False**

Explanation:
Database snapshots capture the state of a database at a specific point in time, offering an effective audit trail for tracking changes.

QUESTION 240
An IS auditor is using a statistical sample to inventory the tape library. What type of test would this be considered?

- **Substantive** (Correct)
- **Compliance**
- **Integrated**
- **Continuous audit**

Explanation:
Using statistical sampling to inventory the tape library is an example of a substantive test, which aims to gather evidence about the completeness and accuracy of an asset inventory.

QUESTION 241
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:

- variable sampling.
- substantive testing.
- **compliance testing.** (Correct)
- stop-or-go sampling.

Section: IS AUDIT PROCESS
Explanation:
Compliance testing is used to verify if controls are being followed in line with policies and procedures. In this case, the IS auditor is testing to ensure that new user accounts are properly authorized, which is a compliance check. Variable sampling relates to numerical estimates, while substantive testing focuses on verifying the integrity of actual transactions. Stop-or-go sampling allows tests to be terminated early, which is not applicable here.

QUESTION 242
The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

- Inherent
- **Detection** (Correct)
- Control
- Business

Section: IS AUDIT PROCESS
Explanation:
Detection risk refers to the risk that the auditor’s procedures will not detect material issues or errors. This risk is directly influenced by the auditor’s choice of audit procedures and techniques. Inherent and control risks are generally outside the auditor's direct influence. Business risk pertains to factors affecting the company, not the audit itself.

QUESTION 243
Overall business risk for a particular threat can be expressed as:

- **a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.** (Correct)
- the magnitude of the impact should a threat source successfully exploit the vulnerability.
- the likelihood of a given threat source exploiting a given vulnerability.
- the collective judgment of the risk assessment team.

Section: IS AUDIT PROCESS
Explanation:
Business risk is best expressed as the combination of both the likelihood of the threat and the magnitude of its impact. The other choices only address part of the equation (either probability or impact), while choice D relies on subjective judgment, which is not scientifically robust.

QUESTION 244
Which of the following is a substantive test?

- Checking a list of exception reports
- Ensuring approval for parameter changes
- **Using a statistical sample to inventory the tape library** (Correct)
- Reviewing password history reports

Section: IS AUDIT PROCESS
Explanation:
Substantive testing focuses on the accuracy and integrity of actual transactions or records, such as verifying the existence of items in the tape library. The other options are examples of compliance tests, which focus on adherence to policies and procedures.

QUESTION 245
Which of the following is a benefit of a risk-based approach to audit planning?

- Audit scheduling may be performed months in advance.
- Budgets are more likely to be met by the IS audit staff.
- Staff will be exposed to a variety of technologies.
- **Resources are allocated to the areas of highest concern.** (Correct)

Section: IS AUDIT PROCESS
Explanation:
The risk-based approach ensures that audit resources are directed to areas with the highest risks, which delivers the most value. Scheduling, budget adherence, and staff exposure are all secondary concerns compared to ensuring that the most critical risks are addressed.

QUESTION 246
An audit charter should:

- be dynamic and change often to coincide with the changing nature of technology and the audit profession.
- clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal controls.
- document the audit procedures designed to achieve the planned audit objectives.
- **outline the overall authority, scope, and responsibilities of the audit function.** (Correct)

Section: IS AUDIT PROCESS
Explanation:
An audit charter defines the audit function’s role, authority, scope, and responsibilities. It provides a high-level framework and typically remains stable over time, with approval from the highest levels of management. Detailed audit objectives, procedures, or frequent changes are not part of an audit charter.

QUESTION 247
The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

- information assets are overprotected.
- a basic level of protection is applied regardless of asset value.
- **appropriate levels of protection are applied to information assets.** (Correct)
- an equal proportion of resources are devoted to protecting all information assets.

Section: IS AUDIT PROCESS
Explanation:
The risk assessment approach ensures that protection is proportional to the value and risk associated with each asset, avoiding over- or under-protection. The baseline approach applies the same level of protection across all assets, regardless of their value or risk level.

QUESTION 248
Which of the following sampling methods is MOST useful when testing for compliance?

- **Attribute sampling** (Correct)
- Variable sampling
- Stratified mean per unit
- Difference estimation

Section: IS AUDIT PROCESS
Explanation:
Attribute sampling is used to test whether a specific control is present or absent in compliance testing. It estimates the rate of occurrence of a specific attribute (e.g., whether a procedure was followed). Variable sampling and the other options are more suited for substantive testing.

QUESTION 249
Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

- **Multiple cycles of backup files remain available.** (Correct)
- Access controls establish accountability for e-mail activity.
- Data classification regulates what information should be communicated via e-mail.
- Within the enterprise, a clear policy for using e-mail ensures that evidence is available.

Section: IS AUDIT PROCESS
Explanation:
E-mail backup files often retain data even after it has been deleted by users, making them a valuable source of evidence for litigation. While access controls and policies help manage e-mail use, the retention of backup files is the primary reason e-mails become useful in legal cases.

QUESTION 250
An IS auditor is assigned to perform a post-implementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:

- **implemented a specific control during the development of the application system.** (Correct)
- designed an embedded audit module exclusively for auditing the application system.
- participated as a member of the application system project team but did not have operational responsibilities.
- provided consulting advice concerning application system best practices.

Section: IS AUDIT PROCESS
Explanation:
Independence is impaired if the IS auditor was directly involved in developing or implementing the system they are reviewing, such as implementing a control. The other activities, such as designing audit modules or giving advice, do not compromise independence as long as the auditor is not operationally responsible.

QUESTION 251
The PRIMARY advantage of a continuous audit approach is that it:

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

Section: IS AUDIT PROCESS
Explanation:
Continuous auditing is particularly beneficial in environments with high transaction volumes and limited physical records, such as time-sharing systems. It allows for ongoing monitoring and quick detection of issues. Continuous auditing often involves collecting evidence during processing, and its complexity depends on the organization’s systems.

QUESTION 252
The PRIMARY purpose of audit trails is to:

- improve response time for users.
- **establish accountability and responsibility for processed transactions.** (Correct)
- improve the operational efficiency of the system.
- provide useful information to auditors who may wish to track transactions.

Section: IS AUDIT PROCESS
Explanation:
Audit trails are primarily used to establish accountability and track responsibility for transactions, helping to ensure that actions can be traced back to specific individuals. While audit trails can be useful to auditors, their primary function is accountability, not operational efficiency.

QUESTION 253
When developing a risk-based audit strategy, an IS auditor should conduct a risk assessment to ensure that:

- controls needed to mitigate risks are in place.
- vulnerabilities and threats are identified.
- **audit risks are considered.** (Correct)
- a gap analysis is appropriate.

Section: IS AUDIT PROCESS
Explanation:
When developing a risk-based audit strategy, understanding risks is essential to ensure the audit covers areas of greatest concern. Controls and gap analyses come after risk identification. Audit risks—risks related to the audit process itself—must be considered to prioritize the audit scope effectively.

QUESTION 254
To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

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

Section: IS AUDIT PROCESS
Explanation:
Developing the audit plan based on a thorough risk assessment ensures that resources are focused on the most critical areas. Scheduling, training, and monitoring are important but secondary to ensuring that the plan addresses the highest risks.

QUESTION 255
An organization's IS audit charter should specify the:

- short- and long-term plans for IS audit engagements.
- objectives and scope of IS audit engagements.
- detailed training plan for the IS audit staff.
- **role of the IS audit function.** (Correct)

Section: IS AUDIT PROCESS
Explanation:
The IS audit charter defines the role, scope, and authority of the audit function within the organization. It provides a high-level view of the audit function’s responsibilities and should be approved by senior management. Planning and training details are managed separately from the charter.

QUESTION 256
An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

- the controls already in place.
- the effectiveness of the controls in place.
- the mechanism for monitoring the risks related to the assets.
- **the threats/vulnerabilities affecting the assets.** (Correct)

Section: IS AUDIT PROCESS
Explanation:
The first step in evaluating a risk assessment is understanding the threats and vulnerabilities that could impact the information systems. Controls and monitoring mechanisms are reviewed later, once the risks are clearly identified.

QUESTION 257
In planning an audit, the MOST critical step is the identification of the:

- **areas of high risk.** (Correct)
- skill sets of the audit staff.
- test steps in the audit.
- time allotted for the audit.

Section: IS AUDIT PROCESS
Explanation:
Identifying the areas of highest risk is the most critical step in audit planning, as it helps ensure that the audit focuses on the most important areas. Other factors, such as skill sets and time, are important but secondary to identifying risks.

QUESTION 258
The extent to which data will be collected during an IS audit should be determined based on the:

- availability of critical and required information.
- auditor's familiarity with the circumstances.

- auditee's ability to find relevant evidence.
- **purpose and scope of the audit being done.** (Correct)

Section: IS AUDIT PROCESS
Explanation:
The extent of data collection in an audit is directly related to the audit’s purpose and scope. An audit with a broad scope will require more data collection than a narrowly focused audit. Familiarity with the situation and the availability of information should not limit the audit’s scope.

QUESTION 259
While planning an audit, an assessment of risk should be made to provide:

- **reasonable assurance that the audit will cover material items.** (Correct)
- definite assurance that material items will be covered during the audit work.
- reasonable assurance that all items will be covered by the audit.
- sufficient assurance that all items will be covered during the audit work.

Section: IS AUDIT PROCESS
Explanation:
An audit risk assessment provides reasonable assurance that material items will be covered during the audit. It helps focus the audit on areas with a higher risk of significant issues. It is unrealistic to expect the audit to cover all items, especially those that are immaterial.

QUESTION 260
An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling when:

- **the probability of error must be objectively quantified.** (Correct)
- the auditor wishes to avoid sampling risk.
- generalized audit software is unavailable.
- the tolerable error rate cannot be determined.

Section: IS AUDIT PROCESS
Explanation:
Statistical sampling allows for the objective quantification of error probabilities, which is necessary when the auditor needs to provide numerical confidence levels. Judgmental sampling, on the other hand, relies on the auditor’s experience but does not offer the same objective measurement. Sampling risk exists in both methods.

QUESTION 261
During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

- A. Address audit objectives
- B. Collect sufficient evidence
- C. Specify appropriate tests
- D. Minimize audit resources

  Correct Answer: A
  Explanation:
  ISACA auditing standards require an IS auditor to plan the audit work to address the audit objectives. The other activities like collecting evidence, specifying tests, or minimizing resources are secondary and serve the main objective of addressing audit objectives.

QUESTION 262
When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

- A. Sufficient evidence will be collected
- B. All significant deficiencies identified will be corrected within a reasonable period
- C. All material weaknesses will be identified
- D. Audit costs will be kept at a minimum level

  Correct Answer: A

Explanation:

An IS auditor should use professional judgment to ensure that sufficient and appropriate evidence will be collected during the audit to support conclusions. Identifying material weaknesses or keeping costs low is important but secondary to collecting enough evidence.

QUESTION 263

An IS auditor evaluating logical access controls should FIRST:

- A. Document the controls applied to the potential access paths to the system
- B. Test controls over the access paths to determine if they are functional
- C. Evaluate the security environment in relation to written policies and practices
- D. Obtain an understanding of the security risks to information processing

Correct Answer: D

Explanation:

The IS auditor should first understand the security risks to information processing by reviewing relevant documentation and conducting a risk assessment. After that, they can document, evaluate, and test the controls.

QUESTION 264

The PRIMARY purpose of an IT forensic audit is:

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

Correct Answer: B

Explanation:

An IT forensic audit focuses on the systematic collection of evidence after a system irregularity. The collected evidence could be used in judicial proceedings if required.

QUESTION 265

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

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

Correct Answer: D

Explanation:

The auditor should expand the sample to gather more evidence before making conclusions. It is essential to determine whether the issue is isolated or systemic before taking further action like issuing a finding or seeking an explanation from management.

QUESTION 266

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

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

Correct Answer: D

Explanation:

Trend/variance detection tools are used to analyze audit trails for anomalies in user or system behavior, making them most suitable for this task.

QUESTION 267

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 desktops
- C. Network monitoring is very limited
- D. Many user IDs have identical passwords

Correct Answer: D

Explanation:

Identical passwords for many user IDs pose the greatest risk since it makes unauthorized access easier. External modems and limited network monitoring are concerns but not as significant as weak password management.

QUESTION 268

Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

- A. The preservation of the chain of custody for electronic evidence
- B. Time and cost savings
- C. Efficiency and effectiveness
- D. Ability to search for violations of intellectual property rights

Correct Answer: A

Explanation:

The primary purpose of forensic software is to ensure the preservation of the chain of custody for electronic evidence. Time and cost savings, efficiency, and specific searches are additional benefits but not the main purpose.

QUESTION 269

An IS auditor has imported data from the client's database. The next step, confirming whether the imported data are complete, is performed by:

- A. Matching control totals of the imported data to control totals of the original data
- B. Sorting the data to confirm whether the data are in the same order as the original data
- C. Reviewing the printout of the first 100 records of original data with the first 100 records of imported data
- D. Filtering data for different categories and matching them to the original data

Correct Answer: A

Explanation:

Matching control totals of the imported data with those of the original data ensures the completeness of the imported data. Sorting or reviewing a subset of records doesn't guarantee completeness across the entire dataset.

QUESTION 270

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

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

Correct Answer: B

Explanation:

Generalized audit software is suitable for performing data analysis to recompute payrolls and detect overpayments. Test data and integrated test facility are more focused on testing controls rather than identifying specific errors from the past.

QUESTION 271
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

- A. Create the procedures document
- B. Terminate the audit
- C. Conduct compliance testing
- D. Identify and evaluate existing practices

Correct Answer: D
Explanation:
The auditor should identify and evaluate the existing security practices rather than create documentation, which could compromise independence. Terminating the audit is premature, and compliance testing is irrelevant if there are no documented procedures.

QUESTION 272
In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

- A. Identify and assess the risk assessment process used by management
- B. Identify information assets and the underlying systems
- C. Disclose the threats and impacts to management
- D. Identify and evaluate the existing controls

Correct Answer: D
Explanation:
Once threats and potential impacts are identified, the auditor's next step is to identify and evaluate the existing controls to mitigate these risks.

QUESTION 273
Which of the following should be of MOST concern to an IS auditor?

- A. Lack of reporting of a successful attack on the network
- B. Failure to notify police of an attempted intrusion
- C. Lack of periodic examination of access rights
- D. Lack of notification to the public of an intrusion

Correct Answer: A
Explanation:
The most critical concern is the lack of reporting of a successful attack since it may hinder timely response and remediation. While notifying police and periodic review of access rights are important, failing to report an attack has greater implications.

QUESTION 274
Which of the following would normally be the MOST reliable evidence for an auditor?

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

Correct Answer: A
Explanation:
Third-party confirmations are considered the most reliable source of evidence. Assurance from management or data from the web is less reliable compared to independent third-party verification.

QUESTION 275

When evaluating the collective effect of preventive, detective, or corrective controls within a process, an IS auditor should be aware of which of the following?

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

Correct Answer: A

Explanation:

An IS auditor should focus on when and where controls are applied in a process as data flows through the system. Understanding this helps in evaluating the effectiveness of the controls.

QUESTION 276

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

Correct Answer: C

Explanation:

Observation and interviews provide the best evidence regarding segregation of duties because they allow the auditor to directly assess what tasks staff members perform.

QUESTION 277

During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

- A. Test data to validate data input
- B. Test data to determine system sort capabilities
- C. Generalized audit software to search for address field duplications
- D. Generalized audit software to search for account field duplications

Correct Answer: C

Explanation:

Generalized audit software can be used to search for address field duplications, which would reveal multiple records for the same customer. Address fields are more likely to remain consistent compared to first names, which may vary in format.

QUESTION 278

Which of the following is an advantage of the program evaluation and review technique (PERT) over the critical path method (CPM)?

- A. PERT considers different scenarios for activity completion
- B. PERT deals with known activities and definite completion time
- C. CPM considers different scenarios for activity completion
- D. CPM evaluates the amount of buffer needed for resources

Correct Answer: A

Explanation:

PERT is designed to handle uncertainty in project schedules by considering different scenarios for activity completion times (optimistic, pessimistic, and most likely). CPM, on the other hand, assumes definite activity times and is better suited for projects with well-known, predictable tasks.

QUESTION 279

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

- A. User management coordination does not exist
- B. Specific user accountability cannot be established
- C. Audit recommendations may not be implemented
- D. Users may have unauthorized access to originate, modify, or delete data

  Correct Answer: D

  Explanation:

  The greatest risk of inadequate data ownership policies is that users may have unauthorized access to data, allowing them to originate, modify, or delete it, which could compromise data integrity and security. Lack of accountability, poor management coordination, or unimplemented audit recommendations are also concerns but secondary.

QUESTION 280

Which of the following risks could result from inadequate software baselining?

- A. Scope creep
- B. Sign-off delays
- C. Software integrity violations
- D. Inadequate controls

  Correct Answer: A

  Explanation:

  Inadequate software baselining can lead to scope creep, where uncontrolled changes to a project can cause it to grow beyond its intended limits. Baselining helps in managing and controlling changes, ensuring that any additions or modifications are properly reviewed and approved.

QUESTION 281

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

Correct Answer: D

Explanation:

Evidence obtained from outside sources is typically more reliable than that from internal sources. A confirmation letter from an external party, like a bank or supplier, offers independent verification, making it highly trustworthy. Oral statements, internal reports, and auditor-conducted tests lack this external objectivity.

QUESTION 282

An IS auditor reviews an organizational chart PRIMARILY for:

- A. an understanding of workflows.
- B. investigating various communication channels.
- C. understanding the responsibilities and authority of individuals.
- D. investigating the network connected to different employees.

Correct Answer: C

Explanation:

The primary purpose of reviewing an organizational chart is to understand the responsibilities and authority of individuals within the organization. This is essential to assess proper segregation of duties. Workflow details and communication channels are secondary concerns and are better analyzed through other tools like workflow charts or network diagrams.

QUESTION 283

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

Correct Answer: A
Explanation:
The availability of online network documentation is a feature beneficial to users, ensuring that necessary information is accessible for troubleshooting or learning. Other options like performance management or interuser communications are network operating system functions but are not directly related to user features.

QUESTION 284
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 schedules.
- D. review data file access records to test the librarian function.

Correct Answer: B
Explanation:
Interviewing programmers can provide direct insight into the actual procedures being followed to restrict access to program documentation. Other options like reviewing file access records or retention plans may help, but they do not offer as much clarity on current practices.

QUESTION 285
Which of the following is an advantage of an integrated test facility (ITF)?

- A. It uses actual master files or dummies, and the IS auditor does not have to review the source of the transaction.
- B. Periodic testing does not require separate test processes.
- C. It validates application systems and tests the ongoing operation of the system.
- D. The need to prepare test data is eliminated.

Correct Answer: B
Explanation:
An ITF allows test transactions to be processed in live systems without interrupting operations, making periodic testing easier and eliminating the need for separate test environments. However, test data still needs to be isolated from live data to ensure no real impact.

QUESTION 286
An IS auditor evaluates the test results of a modification to a system that deals with payment computation. The auditor finds that 50% of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?

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

Correct Answer: C
Explanation:
The auditor should first confirm the errors by examining test cases. Once the discrepancies are confirmed, further investigation can take place. Reporting on findings should only be done after all calculations and test cases have been reviewed.

QUESTION 287
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 totals
- C. preparing simulated transactions for processing and comparing the results to predetermined results
- D. automatic flowcharting and analysis of the source code of the calculation programs

Correct Answer: C
Explanation:
Simulated transactions, where the results are compared with predetermined outcomes, offer the most reliable way to verify the accuracy of tax calculations. Reviewing source code or flowcharting is less effective for detecting specific errors in calculations.

QUESTION 288
An IS auditor performing a review of an application's controls would evaluate the:

- A. efficiency of the application in meeting the business processes
- B. impact of any exposures discovered
- C. business processes served by the application
- D. application's optimization

Correct Answer: B
Explanation:
The primary goal of an application control review is to assess the control mechanisms and identify any exposures or risks related to weaknesses. Other factors like efficiency or optimization are important, but they fall outside the scope of a control-focused audit.

QUESTION 289
In an audit of an inventory application, which approach would provide the BEST evidence that purchase orders are valid?

- A. Testing whether inappropriate personnel can change application parameters
- B. Tracing purchase orders to a computer listing
- C. Comparing receiving reports to purchase order details
- D. Reviewing the application documentation

Correct Answer: A
Explanation:
Testing access controls provides the best assurance that purchase orders are valid by preventing unauthorized personnel from altering system parameters. Tracing or comparing documents only identifies issues after the fact.

QUESTION 290
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

Correct Answer: D
Explanation:
Audit hooks are proactive and allow the auditor to monitor and respond to certain types of transactions as they occur, making them effective for early detection of errors or irregularities.

QUESTION 291
When assessing the design of network monitoring controls, an IS auditor should FIRST review network:

- A. topology diagrams.
- B. bandwidth usage.
- C. traffic analysis reports.
- D. bottleneck locations.

Correct Answer: A

Explanation:

The first step in assessing network monitoring controls is reviewing the network topology diagrams to ensure that the documentation is up to date. Without current and accurate topology diagrams, it would be difficult to effectively monitor the network, identify issues, or manage the network infrastructure.

QUESTION 292

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

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

Correct Answer: C

Explanation:

The first thing an IS auditor should do upon detecting a virus is to immediately notify the appropriate personnel. It is not the auditor's responsibility to remove the virus or change the system. The response team should be alerted to assess the situation and take the necessary corrective action.

QUESTION 293

A substantive test to verify that tape library inventory records are accurate is:

- A. determining whether bar code readers are installed.
- B. determining whether the movement of tapes is authorized.
- C. conducting a physical count of the tape inventory.
- D. checking if receipts and issues of tapes are accurately recorded.

Correct Answer: C

Explanation:

Conducting a physical count of the tape inventory is a substantive test that provides direct evidence of the accuracy of the inventory records. Other choices, such as checking bar code readers or records, are compliance tests and do not provide the same level of assurance.

QUESTION 294

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.

Correct Answer: C

Explanation:

The primary concern in a forensic investigation is preserving evidence. Proper preservation ensures that the evidence can be used in legal proceedings. Without proper preservation, the evidence may be inadmissible in court. Other steps like analysis and disclosure follow after preservation.

QUESTION 295

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 audits.
- D. suspend the audit.

Correct Answer: B

Explanation:

If there are inconsistencies between the payroll clerk's answers and documented procedures, the auditor should expand the scope of testing to include additional substantive tests. This will help to verify whether controls are adequate. It is premature to conclude that controls are inadequate or to suspend the audit without further investigation.

QUESTION 296

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

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

Correct Answer: A

Explanation:

By recommending a specific vendor product, the IS auditor compromises their professional independence. Auditors should avoid endorsing specific vendors to maintain objectivity. Organizational independence and technical/professional competence are important but are not at issue here.

QUESTION 297

The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

- A. understand the business process.
- B. comply with auditing standards.
- C. identify control weakness.
- D. plan substantive testing.

Correct Answer: A

Explanation:

The primary purpose of a functional walkthrough is to understand the business processes and systems under audit. This allows the auditor to gain a better understanding of the environment, which is essential for planning the rest of the audit. Identifying control weaknesses and planning substantive tests come later in the audit process.

QUESTION 298

In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

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

Correct Answer: A

Explanation:

Source code comparison software allows an IS auditor to independently verify program changes without needing detailed information from IS personnel. It compares the control copy with the current version to identify differences and confirm that only authorized changes have been made.

QUESTION 299

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 issues.
- B. gain agreement on the findings.
- C. receive feedback on the adequacy of the audit procedures.
- D. test the structure of the final presentation.

Correct Answer: B

Explanation:

The primary reason for meeting with auditees before closing an audit review is to gain their agreement on the findings. This ensures that there is mutual understanding and acknowledgment of the issues raised. Other options, such as confirming overlooked issues or receiving feedback, are secondary purposes.

QUESTION 300

Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

- A. Test data run
- B. Code review
- C. Automated code comparison
- D. Review of code migration procedures

Correct Answer: C

Explanation:

An automated code comparison is the most efficient and effective technique for detecting unauthorized program changes. It directly compares the current and previous versions of the program to identify any unauthorized alterations. Test data runs and code reviews are less efficient and do not directly address unauthorized changes.

QUESTION 301

Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

A. Include the statement of management in the audit report.
B. Identify whether such software is, indeed, being used by the organization.
C. Reconfirm with management the usage of the software.
D. Discuss the issue with senior management since reporting this could have a negative impact on the organization.

Correct Answer: B

Explanation: The IS auditor must gather sufficient evidence before reporting the use of unlicensed software. Simply relying on management's claims is not enough; independent verification is required to maintain objectivity.

QUESTION 302

While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

A. Audit trail of the versioning of the work papers.
B. Approval of the audit phases.
C. Access rights to the work papers.
D. Confidentiality of the work papers.

Correct Answer: D

Explanation: Encryption is essential to ensure the confidentiality of sensitive electronic work papers. Without encryption, they are vulnerable to unauthorized access.

QUESTION 303

The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

A. Comply with regulatory requirements.
B. Provide a basis for drawing reasonable conclusions.
C. Ensure complete audit coverage.
D. Perform the audit according to the defined scope.
Correct Answer: B
Explanation: The purpose of gathering evidence is to support the audit conclusions. This helps in identifying and validating control weaknesses.

QUESTION 304
After initial investigation, an IS auditor has reasons to believe that fraud may be present. The IS auditor should:
A. Expand activities to determine whether an investigation is warranted.
B. Report the matter to the audit committee.
C. Report the possibility of fraud to top management and ask how they would like to proceed.
D. Consult with external legal counsel to determine the course of action to be taken.
Correct Answer: A
Explanation: The IS auditor must evaluate fraud indicators further before recommending a formal investigation, ensuring that the fraud suspicion is substantial.

QUESTION 305
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)
Correct Answer: B
Explanation: GAS allows for a comprehensive review of all records and can easily identify duplicate invoices, which sampling methods or other tests might miss.

QUESTION 306
Which of the following would be the MOST effective audit technique for identifying segregation of duties violations in a new ERP implementation?
A. Reviewing a report of security rights in the system
B. Reviewing the complexities of authorization objects
C. Building a program to identify conflicts in authorization
D. Examining recent access rights violation cases
Correct Answer: C
Explanation: Developing a program that can systematically identify authorization conflicts is the most efficient and effective way to identify segregation of duties violations in an ERP system.

QUESTION 307
Which of the following would an IS auditor use to determine if unauthorized modifications were made to production programs?
A. System log analysis
B. Compliance testing
C. Forensic analysis
D. Analytical review
Correct Answer: B
Explanation: Compliance testing helps verify whether the change management process was followed consistently and only authorized changes were made to production programs.

QUESTION 308
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 process.
B. Gain more assurance on the findings through root cause analysis.
C. Recommend that program migration be stopped until the change process is documented.
D. Document the finding and present it to management.
Correct Answer: B
Explanation: Before making recommendations, the auditor must ensure that the incidents were indeed due to deficiencies in the change management process and not another cause.

QUESTION 309
During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?
A. Dumping the memory content to a file
B. Generating disk images of the compromised system
C. Rebooting the system
D. Removing the system from the network
Correct Answer: C
Explanation: Rebooting a compromised system can change the system state and potentially destroy evidence, especially in volatile memory.

QUESTION 310
An IS auditor who was involved in designing an organization's business continuity plan (BCP) has been assigned to audit the plan. The IS auditor should:
A. Decline the assignment.
B. Inform management of the possible conflict of interest after completing the audit assignment.
C. Inform the business continuity planning (BCP) team of the possible conflict of interest prior to beginning the assignment.
D. Communicate the possibility of conflict of interest to management prior to starting the assignment.
Correct Answer: D
Explanation: It is important to disclose any potential conflicts of interest, like involvement in the design of the BCP, to management before proceeding with the audit.

QUESTION 311
An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?
A. Personally delete all copies of the unauthorized software.
B. Inform the auditee of the unauthorized software, and follow up to confirm deletion.
C. Report the use of the unauthorized software and the need to prevent recurrence to auditee management.
D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.
Correct 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.

QUESTION 312
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 findings.
B. Not include the finding in the final report, because the audit report should include only unresolved findings.
C. Not include the finding in the final report, because corrective action can be verified by the IS auditor during the audit.
D. Include the finding in the closing meeting for discussion purposes only.

Correct 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.

QUESTION 313
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.
Correct Answer: C
Explanation: Individually the weaknesses are minor; however, together they have the potential to substantially weaken the overall control structure.

QUESTION 314
During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:
A. Ask the auditee to sign a release form accepting full legal responsibility.
B. Elaborate on the significance of the finding and the risks of not correcting it.
C. Report the disagreement to the audit committee for resolution.
D. Accept the auditee's position since they are the process owners.
Correct Answer: B
Explanation: If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risks and exposures, as the auditee may not fully appreciate the magnitude of the exposure.

QUESTION 315
When preparing an audit report, the IS auditor should ensure that the results are supported by:
A. Statements from IS management.
B. Workpapers of other auditors.
C. An organizational control self-assessment.
D. Sufficient and appropriate audit evidence.
Correct Answer: D
Explanation: ISACA's standard on 'reporting' requires the IS auditor to have sufficient and appropriate audit evidence to support the reported results.

QUESTION 316
The final decision to include a material finding in an audit report should be made by the:
A. Audit committee.
B. Auditee's manager.
C. IS auditor.
D. CEO of the organization.
Correct Answer: C
Explanation: The IS auditor should make the final decision about what to include or exclude from the audit report to maintain independence.

QUESTION 317
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. Is a cost-effective way to conduct a comprehensive audit.

C. Engages staff in the risk management process.
D. Reduces the need for external audits.
Correct Answer: C
Explanation: Engaging staff in the risk management process is a significant advantage of using CSA techniques. It enhances accountability and promotes a control-conscious culture.

QUESTION 318
Which of the following would an IS auditor recommend for ensuring compliance with privacy regulations?
A. Conducting periodic employee training on data protection.
B. Using encryption technology for all sensitive data.
C. Implementing a data classification policy.
D. Establishing an incident response plan.
Correct Answer: A
Explanation: Regular training helps ensure that employees are aware of privacy regulations and the organization's policies, making them more effective at compliance.

QUESTION 319
An IS auditor is preparing an audit report on an application under development. Which of the following aspects should be emphasized as the MOST important?
A. That the project is on schedule.
B. That proper change management processes are followed.
C. That the application meets the user requirements.
D. That the application is developed using a formal methodology.
Correct Answer: B
Explanation: Emphasizing proper change management is crucial in development projects, as it mitigates risks associated with unauthorized changes.

QUESTION 320
An IS auditor has identified that an organization's firewall is configured to allow outbound traffic on all ports. What is the MOST significant risk associated with this configuration?
A. Exposure to external threats.
B. Data leakage.
C. Misconfiguration of security policies.
D. Increased administrative overhead.
Correct Answer: B
Explanation: Allowing unrestricted outbound traffic significantly increases the risk of data leakage, as sensitive information could be exfiltrated easily without appropriate controls.

QUESTION 321
An IT steering committee should review information systems PRIMARILY to assess:

- A. whether IT processes support business requirements.
- B. if proposed system functionality is adequate.
- C. the stability of existing software.
- D. the complexity of installed technology.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: The primary role of an IT steering committee is to ensure that the IS department aligns with the organization's mission and objectives. This involves assessing whether IT processes support business requirements. The other options are too narrow in scope.

QUESTION 322

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 objectives.
- D. an absence of control over technology contracts.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The absence of a senior management commitment can lead to misalignment between IT and organizational strategy, increasing the risk of IT projects not meeting business objectives.

QUESTION 323
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

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The IS steering committee primarily serves as a review board for major IS projects, approving and monitoring their progress without becoming involved in routine operations.

QUESTION 324
An IS steering committee should:

- A. include a mix of members from different departments and staff levels.
- B. ensure that IS security policies and procedures have been executed properly.
- C. have formal terms of reference and maintain minutes of its meetings.
- D. be briefed about new trends and products at each meeting by a vendor.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Maintaining detailed minutes is crucial for documenting decisions and activities. This accountability is important for informing the board of directors about the committee's actions.

QUESTION 325
Involvement of senior management is MOST important in the development of:

- A. strategic plans.
- B. IS policies.
- C. IS procedures.
- D. standards and guidelines.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Senior management involvement is critical to ensure that strategic plans align with organizational goals and objectives.

QUESTION 326
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.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: IT governance requires that IT and business strategies are aligned to support the organization’s goals.

QUESTION 327
Establishing the level of acceptable risk is the responsibility of:

- A. quality assurance management.
- B. senior business management.
- C. the chief information officer.
- D. the chief security officer.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Senior management is responsible for establishing acceptable risk levels due to their accountability for organizational operations.

QUESTION 328
IT governance is PRIMARILY the responsibility of the:

- A. chief executive officer.
- B. board of directors.
- C. IT steering committee.
- D. audit committee.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: IT governance is the responsibility of the board of directors, who provide strategic direction and oversight.

QUESTION 329
As an outcome of information security governance, strategic alignment provides:

- A. security requirements driven by enterprise requirements.
- B. baseline security following best practices.
- C. institutionalized and commoditized solutions.
- D. an understanding of risk exposure.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Strategic alignment ensures that security requirements are aligned with the overall enterprise goals and objectives.

QUESTION 330
Which of the following IT governance best practices improves strategic alignment?

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

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Top management mediation is essential for ensuring that IT strategies align with business needs and objectives.

QUESTION 331
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.

Correct Answer: D
Section: IT GOVERNANCE
Explanation: IT governance must align IT strategies with organizational goals, ensuring IT supports and extends those objectives.

QUESTION 332
Which of the following is the MOST important element for the successful implementation of IT governance?

- A. Implementing an IT scorecard
- B. Identifying organizational strategies
- C. Performing a risk assessment
- D. Creating a formal security policy

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Identifying organizational strategies is crucial for aligning IT governance with business objectives.

QUESTION 333
The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

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

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The alignment of IT projects with the business plan is critical for funding and prioritizing IT initiatives.

QUESTION 334
When implementing an IT governance framework in an organization, the MOST important objective is:

- A. IT alignment with the business.
- B. accountability.
- C. value realization with IT.
- D. enhancing the return on IT investments.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: The primary goal of IT governance is to ensure that IT aligns with the organization’s strategic objectives.

QUESTION 335
The ultimate purpose of IT governance is to:

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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: IT governance aims to optimize the use of IT resources to support business objectives, not necessarily to reduce costs or centralize/decentralize resources.

QUESTION 336
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

Correct Answer: B
Section: IT GOVERNANCE
Explanation: The IT balanced scorecard is established at the Defined level (level 3) of the IT governance maturity model.

QUESTION 337
Responsibility for the governance of IT should rest with the:

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

Correct Answer: D
Section: IT GOVERNANCE
Explanation: The ultimate accountability for IT governance resides with the board of directors, who set strategic direction and oversight.

QUESTION 338
An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

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

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Implementing data governance practices will standardize definitions and improve consistency in reporting across departments.

QUESTION 339
From a control perspective, the key element in job descriptions is that they:

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

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Job descriptions are essential for establishing accountability and responsibility, which are crucial from a control perspective.

QUESTION 340
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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Background screening is the most reliable method for verifying the integrity of prospective employees.

QUESTION 341

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

A. Hand over all of the employee's files to another designated employee.

B. Complete a backup of the employee's work.

C. Notify other employees of the termination.

D. Disable the employee's logical access.

Correct Answer: D

Section: IT GOVERNANCE

Explanation: Disabling the terminated employee's logical access is critical to prevent potential misuse of access rights.

QUESTION 342

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

A. Ensure the employee maintains a good quality of life, which will lead to greater productivity.

B. Reduce the opportunity for an employee to commit an improper or illegal act.

C. Provide proper cross-training for another employee.

D. Eliminate the potential disruption caused when an employee takes vacation one day at a time.

Correct Answer: B

Section: IT GOVERNANCE

Explanation: Mandatory vacations help reduce the opportunity for improper or illegal acts by allowing another employee to review the work.

QUESTION 343

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.

Correct Answer: C

Section: IT GOVERNANCE

Explanation: A LAN administrator should not have programming responsibilities to prevent conflicts of interest.

QUESTION 344

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

A. Length of service, since this will help ensure technical competence.

B. Age, as training in audit techniques may be impractical.

C. IS knowledge, since this will bring enhanced credibility to the audit function.

D. Ability, as an IS auditor, to be independent of existing IS relationships.

Correct Answer: D

Section: IT GOVERNANCE

Explanation: The candidate's ability to maintain independence is crucial for effective auditing.

QUESTION 345

An IS auditor should be concerned when a telecommunication analyst:

A. Monitors systems performance and tracks problems resulting from program changes.

B. Reviews network load requirements in terms of current and future transaction volumes.

C. Assesses the impact of the network load on terminal response times and network data transfer rates.

D. Recommends network balancing procedures and improvements.

Correct Answer: A

Section: IT GOVERNANCE

Explanation: Monitoring system performance puts the analyst in a self-monitoring role, which can compromise objectivity.

QUESTION 346

When segregation of duties concerns exist between IT support staff and end users, what would be a suitable compensating control?

A. Restricting physical access to computing equipment

B. Reviewing transaction and application logs

C. Performing background checks prior to hiring IT staff

D. Locking user sessions after a specified period of inactivity

Correct Answer: B

Section: IT GOVERNANCE

Explanation: Reviewing logs directly addresses the threat posed by inadequate segregation of duties.

QUESTION 347

An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

A. Dependency on a single person.

B. Inadequate succession planning.

C. One person knowing all parts of a system.

D. A disruption of operations.

Correct Answer: C

Section: IT GOVERNANCE

Explanation: Assessing the risk of any single employee knowing all parts of a system is critical to identifying potential exposures.

QUESTION 348

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

Correct Answer: D

Section: IT GOVERNANCE

Explanation: Compensating controls are essential to mitigate risks when segregation of duties is not feasible.

QUESTION 349

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

Correct Answer: C

Section: IT GOVERNANCE

Explanation: Security awareness programs educate users, making them less susceptible to social engineering.

QUESTION 350

Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

A. Deleting database activity logs

B. Implementing database optimization tools

C. Monitoring database usage

D. Defining backup and recovery procedures

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Deleting activity logs should be done by someone other than the DBA to ensure proper segregation of duties.

QUESTION 351
To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:
A. Enterprise data model.
B. IT balanced scorecard (BSC).
C. IT organizational structure.
D. Historical financial statements.
Correct Answer: B
Section: IT GOVERNANCE
Explanation: The IT balanced scorecard links IT objectives to business objectives, providing insight into IT investment management.

QUESTION 352
Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?
A. Senior management is aware of critical information assets and demonstrates adequate concern for their protection.
B. Job descriptions contain clear statements of accountability for information security.
C. In accordance with the degree of risk and business impact, there is adequate funding for security efforts.
D. No actual incidents have occurred that have caused a loss or public embarrassment.
Correct Answer: B
Section: IT GOVERNANCE
Explanation: Including security responsibilities in job descriptions ensures staff awareness of their roles regarding information security.

QUESTION 353
Which of the following is a risk of cross-training?
A. Increases the dependence on one employee
B. Does not assist in succession planning
C. One employee may know all parts of a system
D. Does not help in achieving a continuity of operations
Correct Answer: C
Section: IT GOVERNANCE
Explanation: Cross-training may lead to a situation where one individual knows all aspects of a system, increasing risk exposure.

QUESTION 354
Which of the following is normally a responsibility of the chief security officer (CSO)?
A. Periodically reviewing and evaluating the security policy
B. Executing user application and software testing and evaluation
C. Granting and revoking user access to IT resources
D. Approving access to data and applications
Correct Answer: A
Section: IT GOVERNANCE
Explanation: The CSO is responsible for ensuring that security policies are adequate to protect company assets.

QUESTION 355
To support an organization's goals, an IS department should have:

A. A low-cost philosophy.
B. Long- and short-range plans.
C. Leading-edge technology.
D. Plans to acquire new hardware and software.
Correct Answer: B
Section: IT GOVERNANCE
Explanation: Long- and short-range plans should align with organizational goals to effectively support them.

QUESTION 356
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 projects.
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.
Correct Answer: A
Section: IT GOVERNANCE
Explanation: Integration of IS and business staff within projects is critical for successful tactical planning.

QUESTION 357
Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?
A. Allocating resources
B. Keeping current with technology advances
C. Conducting control self-assessment
D. Evaluating hardware needs
Correct Answer: A
Section: IT GOVERNANCE
Explanation: Allocating resources is crucial in short-term planning to align IT investments with management strategies.

QUESTION 358
Which of the following goals would you expect to find in an organization's strategic plan?
A. Test a new accounting package.
B. Perform an evaluation of information technology needs.
C. Implement a new project planning system within the next 12 months.
D. Become the supplier of choice for the product offered.
Correct Answer: D
Section: IT GOVERNANCE
Explanation: Strategic planning focuses on long-term objectives; thus, becoming a preferred supplier represents a significant business goal.

QUESTION 359
Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:
A. Has been approved by line management.
B. Does not vary from the IS department's preliminary budget.
C. Complies with procurement procedures.
D. Supports the business objectives of the organization.
Correct Answer: D
Section: IT GOVERNANCE
Explanation: The IS strategy must align with the organization's business objectives to be deemed effective.

QUESTION 360

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

A. The existing IT environment.

B. The IT governance structure.

C. The overall corporate strategy.

D. The current IT budget.

Correct Answer: C

Section: IT GOVERNANCE

Explanation: Understanding the overall corporate strategy provides context for evaluating the effectiveness of the IT strategic plan.

QUESTION 361

When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

- A. has all the personnel and equipment it needs.
- **B. plans are consistent with management strategy.**
- C. uses its equipment and personnel efficiently and effectively.
- D. has sufficient excess capacity to respond to changing directions.

Correct Answer: B

Section: IT GOVERNANCE

Explanation: Determining if the IS plan is consistent with management strategy relates IS/IT planning to business plans. Choices A, C, and D are effective methods for determining the alignment of IS plans with business objectives and the organization's strategies.

QUESTION 362

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

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

Correct Answer: B

Section: IT GOVERNANCE

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

QUESTION 363

To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

- A. control self-assessments.
- B. a business impact analysis.
- **C. an IT balanced scorecard.**
- D. business process reengineering.

Correct Answer: C

Section: IT GOVERNANCE

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

QUESTION 364

When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

- A. incorporates state of the art technology.
- B. addresses the required operational controls.
- **C. articulates the IT mission and vision.**
- D. specifies project management practices.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls, or project management practices.

QUESTION 365

When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

- A. establishment of a review board.
- B. creation of a security unit.
- **C. effective support of an executive sponsor.**
- D. selection of a security process owner.

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

QUESTION 366

When reviewing an organization's strategic IT plan, an IS auditor should expect to find:

- **A. an assessment of the fit of the organization's application portfolio with business objectives.**
- B. actions to reduce hardware procurement cost.
- C. a listing of approved suppliers of IT contract resources.
- D. a description of the technical architecture for the organization's network perimeter security.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions.

QUESTION 367

The advantage of a bottom-up approach to the development of organizational policies is that the policies:

- A. are developed for the organization as a whole.
- **B. are more likely to be derived as a result of a risk assessment.**
- C. will not conflict with overall corporate policy.
- D. ensure consistency across the organization.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: A bottom-up approach begins by defining operational-level requirements and policies, which are derived and implemented as the result of risk assessments. Choices A, C, and D are advantages of a top-down approach for developing organizational policies.

QUESTION 368

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

- A. User management coordination does not exist.
- **B. Specific user accountability cannot be established.**
- C. Unauthorized users may have access to originate, modify or delete data.
- D. Audit recommendations may not be implemented.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that unauthorized users may have access to originate, modify, or delete data.

QUESTION 369
The PRIMARY objective of an audit of IT security policies is to ensure that:

- A. they are distributed and available to all staff.
- **B. security and control policies support business and IT objectives.**
- C. there is a published organizational chart with functional descriptions.
- D. duties are appropriately segregated.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives.

QUESTION 370
The rate of change in technology increases the importance of:

- A. outsourcing the IS function.
- **B. implementing and enforcing good processes.**
- C. hiring personnel willing to make a career within the organization.
- D. meeting user requirements.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Change requires that good change management processes be implemented and enforced.

QUESTION 371
An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

- **A. this lack of knowledge may lead to unintentional disclosure of sensitive information.**
- B. information security is not critical to all functions.
- C. IS audit should provide security training to the employees.
- D. the audit finding will cause management to provide continuous training to staff.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information.

QUESTION 372
The development of an IS security policy is ultimately the responsibility of the:

- A. IS department.
- B. security committee.
- C. security administrator.
- **D. board of directors.**

Correct Answer: D
Section: IT GOVERNANCE

Explanation: Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors.

QUESTION 373

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

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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: A sound IS security policy will most likely outline a response program to handle suspected intrusions.

QUESTION 374

Which of the following should be included in an organization's IS security policy?

- A. A list of key IT resources to be secured
- **B. The basis for access authorization**
- C. Identity of sensitive security features
- D. Relevant software security features

Correct Answer: B
Section: IT GOVERNANCE
Explanation: The security policy provides the broad framework of security, as laid down and approved by senior management.

QUESTION 375

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

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Identification of the applications required across the network should be identified first.

QUESTION 376

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**

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Training is the only choice that is directed at security awareness.

QUESTION 377

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 maintenance of technical controls

Correct Answer: A
Section: IT GOVERNANCE
Explanation: All employees should understand the purpose and implications of the security policy for it to be effective.

QUESTION 378
When reviewing the information security governance framework, an IS auditor should ensure that:

- A. compliance with policies and standards is effectively monitored.
- **B. information security management is aligned with business objectives.**
- C. the organization has adequate resources to support security management.
- D. controls are in place to protect sensitive information.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: The governance framework must be aligned with business objectives; if it is not, information security will not effectively support the business.

QUESTION 379
The PRIMARY objective of security awareness training is to:

- A. comply with regulatory requirements.
- B. define security roles and responsibilities.
- **C. minimize human error.**
- D. ensure that security technology is used properly.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The purpose of security awareness training is to ensure employees understand their responsibilities regarding security and to reduce the risk of security breaches caused by human error.

QUESTION 380
Which of the following is the BEST approach to protect data integrity in a database management system (DBMS)?

- A. Implementing periodic backups.
- **B. Using data encryption and access controls.**
- C. Using transaction logging and recovery methods.
- D. Using redundant systems.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Data encryption and access controls provide the most comprehensive protection for data integrity, as they restrict access to authorized users and protect data from unauthorized changes.

QUESTION 381
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.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Deriving lower-level policies from corporate policies ensures consistency across the organization. A top-down approach does not ensure compliance or guarantee regular reviews.

QUESTION 382

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 teams.
- 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 specifications.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Privacy laws prohibiting the cross-border flow of personally identifiable information would necessitate keeping the data warehouse in-house.

QUESTION 383
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.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Privacy violations are a significant concern as RFID tags can track purchases, potentially linking them to individuals.

QUESTION 384
When developing a security architecture, which of the following steps should be executed FIRST?

- A. Developing security procedures.
- **B. Defining a security policy.**
- C. Specifying an access control methodology.
- D. Defining roles and responsibilities.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Defining a security policy is the first step in building a security architecture, providing a foundation for other steps.

QUESTION 385
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.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Best practice dictates that user IDs should be deactivated immediately upon termination, regardless of the policy timeframe.

QUESTION 386
An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should FIRST verify that the:

- A. technical platforms between the two companies are interoperable.
- **B. parent bank is authorized to serve as a service provider.**

- C. security features are in place to segregate subsidiary trades.
- D. subsidiary can join as a co-owner of this payment system.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Contractual agreements are crucial for shared services, especially in regulated sectors like banking.

QUESTION 387
IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

- **A. desired result or purpose of implementing specific control procedures.**
- B. best IT security control practices relevant to a specific entity.
- C. techniques for securing information.
- D. security policy.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: IT control objectives articulate the desired outcomes for implementing control procedures in IT activities.

QUESTION 388
The initial step in establishing an information security program is the:

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

Correct Answer: C
Section: IT GOVERNANCE
Explanation: A policy statement reflects executive management's intent and support for security, serving as the foundation for the security program.

QUESTION 389
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.**

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Regular reviews and comparisons with best practices are the best indicators of the adequacy of security awareness content.

QUESTION 390
The PRIMARY objective of implementing corporate governance by an organization's management is to:

- **A. provide strategic direction.**
- B. control business operations.
- C. align IT with business.
- D. implement best practices.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Corporate governance aims to provide strategic direction, ensuring that risks are managed and resources utilized effectively.

QUESTION 391

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.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Selecting projects based on expected business benefits and related risks is the most effective way to align with strategic priorities.

QUESTION 392
An example of a direct benefit to be derived from a proposed IT-related business investment is:

- A. enhanced reputation.
- B. enhanced staff morale.
- C. the use of new technology.
- **D. increased market penetration.**

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Direct benefits from IT investments are quantifiable financial benefits, such as increased market penetration.

QUESTION 393
To assist an organization in planning for IT investments, an IS auditor should recommend the use of:

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

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Enterprise architecture helps document IT assets and processes, facilitating understanding and planning for IT investments.

QUESTION 394
A benefit of open system architecture is that it:

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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Open systems allow for components from different vendors to work together due to defined public standards.

QUESTION 395
In the context of effective information security governance, the primary objective of value delivery is to:

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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Value delivery aims to ensure security investments are optimized to align with business objectives.

QUESTION 396
Which of the following BEST supports the prioritization of new IT projects?

- A. Internal control self-assessment (CSA).
- B. Information systems audit.
- **C. Investment portfolio analysis.**
- D. Business risk assessment.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Investment portfolio analysis clarifies investment strategy and justifies project prioritization.

QUESTION 397
After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

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

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Lack of centralized resource allocation in independent projects increases the risk of misestimating resource availability.

QUESTION 398
Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

- A. Ensuring that invoices are paid to the provider.
- B. Participating in systems design with the provider.
- C. Renegotiating the provider's fees.
- **D. Monitoring the outsourcing provider's performance.**

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Monitoring the provider's performance is crucial to ensure services meet contractual obligations.

QUESTION 399
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, to assess the potential risks associated with outsourcing.**
- B. No, it is inappropriate as it could compromise the vendor's confidentiality.
- C. No, it is unnecessary since IS processing is not a critical function.
- D. Yes, but only after a formal non-disclosure agreement is signed.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Understanding vendors' business continuity plans is essential to evaluate risks and ensure preparedness.

QUESTION 400

An organization wants to ensure that a new information system is cost-effective. The BEST approach is to:

- A. adopt a vendor solution to minimize integration costs.
- **B. conduct a cost-benefit analysis (CBA) prior to investment.**
- C. purchase the most up-to-date technology.
- D. develop the system in-house to reduce licensing costs.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: A cost-benefit analysis helps evaluate whether expected benefits justify the costs involved.

QUESTION 401

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

- A. There could be a question regarding the legal jurisdiction.
- B. Having a provider abroad will cause excessive costs in future audits.
- C. The auditing process will be difficult because of the distance.
- D. There could be different auditing norms.

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

QUESTION 402

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

Correct Answer: A
Section: IT GOVERNANCE
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.

QUESTION 403

To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

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

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Gain-sharing performance bonuses provide a financial incentive for the outsourcer to exceed the stated contract terms and can lead to cost savings for the client.

QUESTION 404

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

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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Accountability cannot be transferred to external parties. Choices B, C, and D can be performed by outside entities as long as accountability remains within the organization.

QUESTION 405
An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine FIRST?

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

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The complexity of IT structures matched by the complexity and interplay of responsibilities and warranties may affect or void the effectiveness of those warranties and the reasonable certainty that the business needs will be met.

QUESTION 406
With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?

- A. Outsourced activities are core and provide a differentiated advantage to the organization.
- B. Periodic renegotiation is specified in the outsourcing contract.
- C. The outsourcing contract fails to cover every action required by the arrangement.
- D. Similar activities are outsourced to more than one vendor.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: An organization's core activities generally should not be outsourced because they are what the organization does best; an IS auditor observing that should be concerned.

QUESTION 407
While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern should be that the:

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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: The potential risk that the confidentiality of the information will be compromised is the primary concern in this scenario.

QUESTION 408
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

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Contractual requirements are one of the sources that should be consulted to identify the requirements for the management of information assets.

QUESTION 409
An organization has outsourced its help desk activities. An IS auditor's GREATEST concern when reviewing the contract and associated service level agreement (SLA) between the organization and vendor should be the provisions for:

- A. documentation of staff background checks.
- B. independent audit reports or full audit access.
- C. reporting the year-to-year incremental cost reductions.
- D. reporting staff turnover, development or training.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Ensuring that independent audit reports are available is crucial to verify that the outsourced functions meet the necessary standards.

QUESTION 410
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 standards.
- B. agrees to be subject to external security reviews.
- C. has a good market reputation for service and experience.
- D. complies with security policies of the organization.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: It is critical that an independent security review of an outsourcing vendor be obtained because customer credit information will be kept there.

QUESTION 411
The risks associated with electronic evidence gathering would MOST likely be reduced by an email:

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

Correct Answer: C
Section: IT GOVERNANCE
Explanation: A well-archived email policy allows for specific email records to be retrieved without disclosing other confidential records.

QUESTION 412
The output of the risk management process is an input for making:

- A. business plans.
- B. audit charters.
- C. security policy decisions.
- D. software design decisions.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The risk management process focuses on making security-related decisions, such as the level of acceptable risk.

QUESTION 413
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 applications in development
- C. Identify threats and likelihood of occurrence
- D. Check the budget available for risk management

Correct Answer: C
Section: IT GOVERNANCE
Explanation: After identifying vulnerabilities, the next step is to assess the threats and their likelihood of occurrence.

QUESTION 414
Which of the following is a mechanism for mitigating risks?

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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Risks are mitigated by implementing appropriate security and control practices.

QUESTION 415
When developing a risk management program, what is the FIRST activity to be performed?

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

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Identification of the assets to be protected is the first step in the development of a risk management program.

QUESTION 416
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 assets.
- B. calculate a return on investment (ROI).
- C. apply a qualitative approach.
- D. spend the time needed to define exactly the loss amount.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: When it is difficult to calculate financial losses, a qualitative approach is often the best method to assess potential impact.

QUESTION 417
Which of the following does a lack of adequate security controls represent?

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

Correct Answer: D
Section: IT GOVERNANCE
Explanation: The lack of adequate security controls is considered a vulnerability, exposing information to risks.

QUESTION 418
Assessing IT risks is BEST achieved by:

- A. evaluating threats associated with business processes.
- B. applying regulatory requirements to controls.
- C. calculating the return on investment (ROI) on security controls.
- D. defining and assessing security controls.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Business process assessment helps evaluate threats to information and IT risks, aligning with operational requirements.

QUESTION 419
During an audit, the IS auditor finds that a large number of employees have been accessing files that they have no business reason to view. The BEST recommendation is to implement:

- A. access controls based on business functions.
- B. a monitoring tool to track employee file access.
- C. mandatory training sessions on security policy.
- D. an audit of employee access to critical files.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Implementing access controls based on business functions will help ensure employees can only access files relevant to their roles.

QUESTION 420
In the context of business continuity, the primary purpose of an incident management process is to ensure:

- A. all incidents are managed to minimize their impact on business operations.
- B. training for incident management staff is conducted.
- C. the incident response team is notified quickly.
- D. audits of incident management practices are performed regularly.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: The main objective of incident management is to minimize the impact of incidents on business operations

QUESTION 421
An IS auditor reviewing the risk assessment process of an organization should FIRST:

- **A.** identify the reasonable threats to the information assets.
- **B.** analyze the technical and organizational vulnerabilities.
- **C.** identify and rank the information assets.
- **D.** evaluate the effect of a potential security breach.

Correct Answer: C
Section: IT GOVERNANCE

Explanation: Identification and ranking of information assets set the scope for assessing risk, guiding the analysis of threats and vulnerabilities.

QUESTION 422

An IS auditor is reviewing an IT security risk management program. Measures of security risk should:

- **A.** address all of the network risks.
- **B.** be tracked over time against the IT strategic plan.
- **C.** take into account the entire IT environment.
- **D.** result in the identification of vulnerability tolerances.

Correct Answer: C

Section: IT GOVERNANCE

Explanation: Security risk measures must consider the entire IT environment to prioritize critical areas for risk reduction.

QUESTION 423

Which of the following should be considered FIRST when implementing a risk management program?

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

Correct Answer: A

Section: IT GOVERNANCE

Explanation: Understanding the organization's threat, vulnerability, and risk profile is crucial as a foundational step in risk management.

QUESTION 424

As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

- **A.** performance measurement.
- **B.** strategic alignment.
- **C.** value delivery.
- **D.** resource management.

Correct Answer: A

Section: IT GOVERNANCE

Explanation: Performance measurement provides stakeholders with information on IT performance compared to objectives, ensuring transparency.

QUESTION 425

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.

Correct Answer: C

Section: IT GOVERNANCE

Explanation: Prioritizing areas representing known risks to the enterprise's operations is essential for effective governance implementation.

QUESTION 426

The PRIMARY benefit of implementing a security program as part of a security governance framework is the:

- **A.** alignment of the IT activities with IS audit recommendations.
- **B.** enforcement of the management of security risks.

- **C.** implementation of the chief information security officer's (CISO) recommendations.
- **D.** reduction of the cost for IT security.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: The main benefit is the effective management of security risks and monitoring residual risks post-implementation.

QUESTION 427
An IS auditor who is reviewing incident reports discovers that, in one instance, an important document left on an employee's desk was removed and put in the garbage by the outsourced cleaning staff. Which of the following should the IS auditor recommend to management?

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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Implementing strict controls with the cleaning agency is necessary to prevent unauthorized access to sensitive documents.

QUESTION 428
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 experts.
- **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.

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Regular meetings for risk identification and assessment are vital for managing risks effectively in a medium-sized organization.

QUESTION 429
The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: The IT balanced scorecard focuses on key performance indicators beyond just financial results.

QUESTION 430
Before implementing an IT balanced scorecard, an organization must:

- **A.** deliver effective and efficient services.
- **B.** define key performance indicators.

- **C.** provide business value to IT projects.
- **D.** control IT expenses.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Defining key performance indicators is essential for the successful implementation of an IT balanced scorecard.

QUESTION 431
Which of the following is the PRIMARY objective of an IT performance measurement process?

- **A.** Minimize errors.
- **B.** Gather performance data.
- **C.** Establish performance baselines.
- **D.** Optimize performance.

Correct Answer: D
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: The primary objective is to optimize performance across IT services and products.

QUESTION 432
When auditing the proposed acquisition of a new computer system, an IS auditor should FIRST establish that:

- **A.** a clear business case has been approved by management.
- **B.** corporate security standards will be met.
- **C.** users will be involved in the implementation plan.
- **D.** the new system will meet all required user functionality.

Correct Answer: A
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: A clear business case is essential to ensure the acquisition aligns with business needs.

QUESTION 433
Documentation of a business case used in an IT development project should be retained until:

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

Correct Answer: A
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: The business case should be retained throughout the life cycle for reference and evaluation.

QUESTION 434
Which of the following risks could result from inadequate software baselining?

- **A.** Scope creep.
- **B.** Sign-off delays.
- **C.** Software integrity violations.
- **D.** Inadequate controls.

Correct Answer: A
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: Inadequate baselining can lead to scope creep due to uncontrolled changes during development.

QUESTION 435
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.

Correct Answer: D
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: Lack of adequate user involvement often results in systems that do not meet user needs.

QUESTION 436
Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

- **A.** Function point analysis.
- **B.** PERT chart.
- **C.** Rapid application development.
- **D.** Object-oriented system development.

Correct Answer: B
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: A PERT chart helps in determining project duration by analyzing the tasks and their interdependencies.

QUESTION 437
The reason for establishing a stop or freezing point on the design of a new system is to:

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

Correct Answer: C
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: A freezing point allows for a review of changes to ensure they are cost-effective and justified.

QUESTION 438
Change control for business application systems being developed using prototyping could be complicated by the:

- **A.** iterative nature of prototyping.
- **B.** need for constant user feedback.
- **C.** complexity of the proposed systems.
- **D.** lack of documentation.

Correct Answer: A
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: The iterative nature of prototyping makes it difficult to control changes since prototypes are continuously modified based on feedback.

QUESTION 439
An IS auditor is reviewing the project management practices of a large organization. The organization is implementing a major information system and, at the project's outset, has not established a formal project management process. Which of the following would be the MOST effective recommendation for the organization?

- **A.** Establish a project steering committee.
- **B.** Implement project management software tools.
- **C.** Develop a project charter and project management plan.
- **D.** Hire an external project manager.

Correct Answer: C
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: Establishing a project charter and plan is fundamental to ensure proper project management practices are followed.

QUESTION 440
Which of the following is MOST important to consider when determining whether to convert to an automated system?

- **A.** Cost of system maintenance.
- **B.** Internal controls needed to secure the data.
- **C.** User training requirements.
- **D.** Efficiency of the new system.

Correct Answer: D
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: The efficiency of the new system is crucial to determine whether automation provides a net benefit over current processes.

QUESTION 440
When planning to add personnel to tasks imposing time constraints on the duration of a project, which of the following should be revalidated FIRST?

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

Correct Answer: B
Explanation:
Adding personnel may alter the sequence of activities on the critical path, potentially reducing the overall project duration. The critical path determines the longest stretch of dependent activities, so adding resources must be evaluated against its impact on this path before adjusting the budget, remaining task lengths, or personnel assignments. Other tasks might not be directly impacted since they may have slack time available.

QUESTION 441
Which of the following is a characteristic of timebox management?

- **A.** Not suitable for prototyping or rapid application development (RAD)
- **B.** Eliminates the need for a quality process
- **C.** Prevents cost overruns and delivery delays
- **D.** Separates system and user acceptance testing

Correct Answer: C
Explanation:
Timebox management sets strict boundaries for time and cost, making it suitable for rapid application development (RAD) and preventing cost overruns and delivery delays. It encourages focused work within limited timeframes but does not eliminate the need for a quality process. System and user acceptance testing are integrated, rather than separated.

QUESTION 442
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

Correct Answer: C
Explanation:
A project portfolio database contains data such as project owner, schedules, objectives, type, status, and costs, which are necessary for managing multiple projects. This helps in evaluating the effectiveness of controls. A project database pertains to single projects, while policy documents provide guidance, and program organization defines team roles but does not give a holistic view of project management controls.

QUESTION 443

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

- **A.** As close to their writing (i.e., point of origination) as possible.
- **B.** Primarily at project start-up to ensure that the project is established in accordance with organizational governance standards.
- **C.** Continuously throughout the project with an emphasis on finding and fixing defects primarily during testing to maximize the defect detection rate.
- **D.** Mainly at project close-down to capture lessons learned that can be applied to future projects.

Correct Answer: A

Explanation:

Quality management techniques are most cost-effective when applied early, close to the point of origination. The earlier defects are identified and resolved, the lower the cost of correcting them. Waiting until later phases, such as during testing, increases rework costs. Lessons learned should be captured but applying techniques throughout the project yields better outcomes.

QUESTION 444

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

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

Correct Answer: B

Explanation:

Activities with zero slack time are on the critical path, which determines the overall project duration. Reducing time on these activities, often through paying a premium (crashing), can shorten the total project time. Activities with slack time do not impact the overall project duration and thus are not suitable for speeding up completion.

QUESTION 445

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

Correct Answer: B

Explanation:

A postproject review aims to gather lessons learned for future projects. While assessing risks and verifying controls are important, they are more relevant to the acceptance testing and production phases. Deleting test data is a separate operational procedure, not a key focus of postproject reviews.

QUESTION 446

An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

- **A.** Complexity and risks associated with the project have been analyzed.
- **B.** Resources needed throughout the project have been determined.
- **C.** Project deliverables have been identified.
- **D.** A contract for external parties involved in the project has been completed.

Correct Answer: A

Explanation:

At the project initiation stage, the IS auditor’s main focus should be on ensuring that the complexity and risks have been properly analyzed, as these factors are critical to a project’s success. Other aspects like resources, deliverables, and contracts are important but are determined based on the complexity and risk assessment.

QUESTION 447
An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start impacting the project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

- **A.** Stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plans.
- **B.** Accept the project manager's position as the project manager is accountable for the outcome of the project.
- **C.** Offer to work with the risk manager when one is appointed.
- **D.** Inform the project manager that the IS auditor will conduct a review of the risks at the completion of the requirements definition phase of the project.

Correct Answer: A
Explanation:
The IS auditor should emphasize the importance of early risk identification and documentation, as this is a critical aspect of effective project management. Waiting until risks materialize can lead to project failure, while early risk management allows for mitigation strategies.

QUESTION 448
While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

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

Correct Answer: A
Explanation: To be effective, the quality assurance (QA) function should be independent of project management. The QA function should interact between project management and user management but should not be directly involved with the project implementation team, as that could compromise its independence and effectiveness.

QUESTION 449
When reviewing a project where quality is a major concern, an IS auditor should use the project management triangle to explain that:

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

Correct Answer: A
Explanation: The project management triangle consists of three dimensions: scope, time, and cost. If resource allocation is decreased, quality can still be improved if there is flexibility in extending the project's delivery time. Therefore, adjusting one dimension can impact the others to maintain the balance.

QUESTION 450
An IS auditor is assigned to audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

- A. Report that the organization does not have effective project management.
- B. Recommend the project manager be changed.

- C. Review the IT governance structure.
- **D.** Review the conduct of the project and the business case.

Correct Answer: D
Explanation: The IS auditor should first review the project and its business case to understand the reasons for the time and cost overruns before making recommendations. It's essential to assess the situation fully before concluding whether governance or management issues are present.

QUESTION 451
Which of the following should an IS auditor review to understand project progress in terms of time, budget, and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

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

Correct Answer: B
Explanation: Earned value analysis (EVA) is a widely used method to measure project progress and forecast completion time and costs. EVA compares the planned work with actual work completed to determine if the project is progressing according to plan.

QUESTION 452
When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

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

Correct Answer: B
Explanation: The IS auditor should recommend updating the business case as it is a key input for decision-making during the project's lifecycle. It's important to keep the business case current and reassess the project's value before deciding on any course of action.

QUESTION 453
An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. Of the following, who is PRIMARILY responsible for overseeing the project to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

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

Correct Answer: C
Explanation: The project steering committee is responsible for overseeing the project's progress to ensure it meets business objectives. The project sponsor funds the project but does not oversee daily progress, while the development and user teams focus on specific tasks rather than overall project direction.

QUESTION 454
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

Correct Answer: D
Explanation: The data owner is responsible for ensuring that data migration is complete, accurate, and valid before going live. The IS auditor may verify that this process is followed, but the primary responsibility for data sign-off rests with the data owner.

QUESTION 455
A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

- **A.** what amount of progress against the schedule has been achieved.
- B. if the project budget can be reduced.
- C. if the project could be brought in ahead of schedule.
- D. if the budget savings can be applied to increase the project scope.

Correct Answer: A
Explanation:
The IS auditor should assess the actual progress made relative to the project schedule to understand the relationship between the time elapsed and the budget spent. Spending less than anticipated could be a sign of slow progress, and without knowing the amount of work done, the project's status cannot be properly assessed.

QUESTION 456
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 issues.
- D. recommend that the project manager reallocate test resources to resolve the issues.

Correct Answer: C
Explanation:
The IS auditor should first assess the risks posed by the unresolved audit recommendations. Once the risks are evaluated, management can make informed decisions, such as implementing compensating controls or accepting the risk, if appropriate.

QUESTION 457
Which of the following techniques would BEST help an IS auditor gain reasonable assurance that a project can meet its target date?

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

Correct Answer: C
Explanation:
Extrapolating the overall end date based on completed work packages and current resources gives the IS auditor a realistic estimation of the project's final completion date. This method relies on actual progress, making it more reliable than subjective estimations or calculations based on the budget alone.

QUESTION 458
Which of the following situations would increase the likelihood of fraud?

- **A.** Application programmers are implementing changes to production programs.

- B. Application programmers are implementing changes to test programs.
- C. Operations support staff are implementing changes to batch schedules.
- D. Database administrators are implementing changes to data structures.

Correct Answer: A
Explanation:
Allowing application programmers to implement changes directly to production programs could lead to fraudulent activity. This situation bypasses segregation of duties and introduces the risk of unauthorized modifications to critical applications.

QUESTION 459
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.

Correct Answer: A
Explanation:
A checksum is used to verify the integrity of the data by ensuring that no unauthorized modifications have occurred. It helps detect accidental or intentional data alterations during transmission.

QUESTION 460
Before implementing controls, management should FIRST ensure that the controls:

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

Correct Answer: A
Explanation:
Controls should address specific risk issues effectively. While other factors like cost-benefit analysis and impact on productivity are important, the primary purpose of implementing a control is to mitigate a risk. Hence, management should first ensure that the control addresses the identified risk.

QUESTION 461
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

Correct Answer: B
Explanation:
The transaction journal records all transaction activity, which can be compared to authorized source documents to identify any unauthorized input. The other options either do not capture all terminal activities or are specific to particular types of errors.

QUESTION 462
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

Correct Answer: C
Explanation:
A completeness check ensures that a field contains valid data (i.e., not zeros or blanks). A check digit validates data integrity, an existence check ensures data entry follows predetermined criteria, and a reasonableness check ensures input data fall within expected ranges.

QUESTION 463
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

Correct Answer: D
Explanation:
Data should be edited and validated at the remote site before transmission to the central site to prevent erroneous or incomplete data from entering the central system.

QUESTION 464
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

Correct Answer: A
Explanation:
Control totals should be implemented during data preparation, as it is the earliest opportunity to establish data integrity before processing begins.

QUESTION 465
Functional acknowledgements are used:

- **A.** As an audit trail for EDI transactions
- **B.** To functionally describe the IS department
- **C.** To document user roles and responsibilities
- **D.** As a functional description of application software

Correct Answer: A
Explanation:
Functional acknowledgements in EDI transactions confirm the receipt of electronic documents, which serves as an audit trail. The other choices are unrelated to functional acknowledgements.

QUESTION 466
A proposed transaction processing application will have many data capture sources and outputs in paper and electronic form. To ensure that transactions are not lost during processing, an IS auditor should recommend the inclusion of:

- **A.** Validation controls
- **B.** Internal credibility checks
- **C.** Clerical control procedures
- **D.** Automated systems balancing

Correct Answer: D

Explanation:
Automated systems balancing ensures that total inputs match total outputs, alerting the organization to any lost transactions. Other controls help validate data but do not specifically detect lost transactions.

QUESTION 467
What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

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

Correct Answer: B
Explanation:
A base-case system evaluation involves using test data as part of a comprehensive test to verify correct system operations and validate them over time. The other methods focus on specific test types but lack the continuous monitoring element.

QUESTION 468
What control detects transmission errors by appending calculated bits onto the end of each segment of data?

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

Correct Answer: C
Explanation:
A redundancy check appends calculated bits to detect transmission errors. Parity checks are hardware controls, reasonableness checks compare data to predefined limits, and check digits detect transposition or transcription errors.

QUESTION 469
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

Correct Answer: B
Explanation:
A check digit is calculated mathematically and appended to data to ensure its integrity. It is particularly effective in detecting transposition and transcription errors.

QUESTION 470
Which of the following is the GREATEST risk when implementing a data warehouse?

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

Correct Answer: B
Explanation:
Access control deficiencies pose the greatest risk since data in a warehouse should not be modified. Data duplication is inherent in warehousing, and delayed updates are manageable risks, while response times typically don't affect the warehouse environment directly.

QUESTION 471
Which of the following will BEST ensure the successful offshore development of business applications?

- **A.** Stringent contract management practices
- **B.** Detailed and correctly applied specifications
- **C.** Awareness of cultural and political differences
- **D.** Postimplementation reviews

Correct Answer: B
Explanation:
Detailed and correctly applied specifications are essential for offshore development projects to ensure that the business needs are communicated clearly despite any physical or cultural distance. While the other factors are important, well-defined specifications are most critical for success.

QUESTION 472
Which of the following is the GREATEST risk to the effectiveness of application system controls?

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

Correct Answer: C
Explanation:
Collusion between employees poses the greatest risk to system controls because it allows individuals to bypass even well-designed controls. Inadequate manuals or unresolved compliance issues are important but not as impactful as collusion in undermining controls.

QUESTION 473
The MAIN purpose of a transaction audit trail is to:

- **A.** Reduce the use of storage media
- **B.** Determine accountability and responsibility for processed transactions
- **C.** Help an IS auditor trace transactions
- **D.** Provide useful information for capacity planning

Correct Answer: B
Explanation:
A transaction audit trail's main purpose is to ensure accountability and responsibility by tracking the entire transaction process. Although it helps an auditor trace transactions, its primary role is to establish responsibility for the actions taken.

QUESTION 474
An appropriate control for ensuring the authenticity of orders received in an EDI application is to:

- **A.** Acknowledge receipt of electronic orders with a confirmation message
- **B.** Perform reasonableness checks on quantities ordered before filling orders
- **C.** Verify the identity of senders and determine if orders correspond to contract terms
- **D.** Encrypt electronic orders

Correct Answer: C
Explanation:
Verifying the identity of the sender and ensuring the orders match contract terms is critical in an EDI system to confirm authenticity. While encryption and acknowledgment messages are important, they do not ensure authenticity by themselves.

QUESTION 475
A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization, and the system should be capable of identifying errors that require follow-up. Which of the following would BEST meet these objectives?

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

Correct Answer: C

Explanation:

An EDI system provides real-time electronic document exchange between businesses, allowing automation of invoice payments and the ability to identify and resolve errors quickly, fulfilling the firm's objectives. Other options do not provide the same level of automation and efficiency.

QUESTION 476

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 goals
- **C.** A documented process
- **D.** A process tailored to specific projects

Correct Answer: A

Explanation:

The highest level of the CMM is Level 5 (Optimizing), which focuses on continuous improvement of processes. Quantitative quality goals are associated with Level 4 (Managed), and a documented process is a feature of Level 3 (Defined).

QUESTION 477

During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

- **A.** Test the software for compatibility with existing hardware
- **B.** Perform a gap analysis
- **C.** Review the licensing policy
- **D.** Ensure that the procedure had been approved

Correct Answer: D

Explanation:

The IS auditor should first confirm that the procedure followed for acquiring the software was approved by appropriate authorities. This ensures the process aligns with business objectives and established procedures.

QUESTION 478

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

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

Correct Answer: B

Explanation:

Failure during acceptance testing has the greatest impact since it is the final stage before the software is implemented. It would delay the deployment and result in costly fixes. Failures in system, integration, and unit testing occur earlier and are less impactful.

QUESTION 479

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

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

Correct Answer: B

Explanation:

A strength of an IDE is that it provides programmers with enhanced resources and tools, which help in development and testing. The other options are weaknesses that can occur in an IDE environment.

QUESTION 480

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

Correct Answer: A

Explanation:

The quality of the metadata is the most crucial element in a data warehouse, as it defines the structure and meaning of the data. Accurate metadata ensures that users can efficiently query and analyze the data. Transaction speed and data volatility are less critical in this context.

QUESTION 481

Ideally, stress testing should be carried out in a:

- **A.** Test environment using test data
- **B.** Production environment using live workloads
- **C.** Test environment using live workloads
- **D.** Production environment using test data

Correct Answer: C

Explanation:

Stress testing should be conducted in a test environment using live workloads to simulate real-world conditions without affecting the production environment. Testing with live workloads ensures that the system can handle expected traffic and user behavior.

Question 482

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

Correct Answer: C

Explanation: Encapsulation is a property that restricts access to data by only allowing defined methods and properties to interact with it. This enhances security by preventing unauthorized access.

Question 483

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

A. Black box test
B. Desk checking
C. Structured walkthrough
D. Design and code
Correct Answer: A
Explanation: A black box test is a dynamic analysis tool for testing software modules without internal knowledge, relying on input and output results.

Question 484
The phases and deliverables of a system development life cycle (SDLC) project should be determined:
A. During the initial planning stages of the project.
B. After early planning has been completed, but before work has begun.
C. Throughout the work stages, based on risks and exposures.
D. Only after all risks and exposures have been identified and the IS auditor has recommended appropriate controls.
Correct Answer: A
Explanation: Proper project planning, including defining phases and deliverables, is crucial early in the project to ensure success and address risks from the start.

Question 485
Which of the following is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality?
A. Function point analysis
B. Critical path methodology
C. Rapid application development
D. Program evaluation review technique
Correct Answer: C
Explanation: Rapid application development (RAD) focuses on faster delivery of systems, reducing costs and ensuring quality.

Question 486
When implementing an application software package, which of the following presents the GREATEST risk?
A. Uncontrolled multiple software versions
B. Source programs that are not synchronized with object code
C. Incorrectly set parameters
D. Programming errors
Correct Answer: C
Explanation: Incorrectly set parameters can significantly disrupt the functionality of the software, making it the greatest risk during implementation.

Question 487
Which of the following is an advantage of prototyping?
A. The finished system normally has strong internal controls.
B. Prototype systems can provide significant time and cost savings.
C. Change control is often less complicated with prototype systems.
D. It ensures that functions or extras are not added to the intended system.
Correct Answer: B
Explanation: Prototyping can save time and costs by allowing early user feedback and iterative adjustments, but it can also lead to weaker internal controls.

Question 488
A decision support system (DSS):

A. Is aimed at solving highly structured problems.
B. Combines the use of models with nontraditional data access and retrieval functions.
C. Emphasizes flexibility in the decision-making approach of users.
D. Supports only structured decision-making tasks.
Correct Answer: C
Explanation: DSS is designed to be flexible in supporting decision-making, especially for semi-structured or unstructured problems.

Question 489
An advantage of using sanitized live transactions in test data is that:
A. All transaction types will be included.
B. Every error condition is likely to be tested.
C. No special routines are required to assess the results.
D. Test transactions are representative of live processing.
Correct Answer: D
Explanation: Using sanitized live transactions ensures that the test data closely resembles actual production data, making the tests more realistic.

Question 490
An IS auditor's PRIMARY concern when application developers wish to use a copy of yesterday's production transaction file for volume tests is that:
A. Users may prefer to use contrived data for testing.
B. Unauthorized access to sensitive data may result.
C. Error handling and credibility checks may not be fully proven.
D. The full functionality of the new process may not necessarily be tested.
Correct Answer: B
Explanation: Using a live production file poses a risk of exposing sensitive data unless the data is properly sanitized.

Question 491
Which of the following is the PRIMARY purpose for conducting parallel testing?
A. To determine if the system is cost-effective
B. To enable comprehensive unit and system testing
C. To highlight errors in the program interfaces with files
D. To ensure the new system meets user requirements
Correct Answer: D
Explanation: Parallel testing is primarily conducted to verify that the new system meets user requirements by comparing its performance against the existing system.

Question 492
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. Rules
B. Decision trees
C. Semantic nets
D. Dataflow diagrams
Correct Answer: B
Explanation: Decision trees guide users through a series of questions or choices to reach a conclusion, making them a key component of the knowledge base in expert systems.

Question 493
An advantage in using a bottom-up vs. a top-down approach to software testing is that:

A. Interface errors are detected earlier.
B. Confidence in the system is achieved earlier.
C. Errors in critical modules are detected earlier.
D. Major functions and processing are tested earlier.
Correct Answer: C
Explanation: Bottom-up testing identifies errors in critical modules earlier, as testing starts at the program or module level.

Question 494
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
Correct Answer: B
Explanation: During the requirements definition phase, user acceptance test plans are developed to ensure that the system meets user needs.

Question 495
The use of object-oriented design and development techniques would MOST likely:
A. Facilitate the ability to reuse modules.
B. Improve system performance.
C. Enhance control effectiveness.
D. Speed up the system development life cycle.
Correct Answer: A
Explanation: Object-oriented design encourages the reuse of modules, making it easier to repurpose components across different systems or applications.

Question 496
Which of the following should be included in a feasibility study for a project to implement an EDI process?
A. The encryption algorithm format
B. The detailed internal control procedures
C. The necessary communication protocols
D. The proposed trusted third-party agreement
Correct Answer: C
Explanation: Communication protocols must be included in the feasibility study to assess costs and technical risks associated with implementing the EDI process.

Question 497
When a new system is to be implemented within a short time frame, it is MOST important to:
A. Finish writing user manuals.
B. Perform user acceptance testing.
C. Add last-minute enhancements to functionalities.
D. Ensure that the code has been documented and reviewed.
Correct Answer: B
Explanation: User acceptance testing is essential to verify that the system works as intended, especially when time is limited for implementation.

Question 498
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.
Correct Answer: D
Explanation: To ensure future maintenance or updates, the source code should be placed in escrow in case the vendor goes out of business.

Question 499
The MOST likely explanation for the use of applets in an Internet application is that:
A. It is sent over the network from the server.
B. The server does not run the program and the output is not sent over the network.
C. They improve the performance of the web server and network.
D. It is a JAVA program downloaded through the web browser and executed by the web server of the client machine.
Correct Answer: C
Explanation: Applets are small programs that run on the client side, reducing the load on the web server and improving overall network performance.

Question 500
A company has contracted with an external consulting firm to implement a commercial financial system to replace its existing system developed in-house. In reviewing the proposed development approach, which of the following would be of GREATEST concern?
A. Acceptance testing is to be managed by users.
B. A quality plan is not part of the contracted deliverables.
C. Not all business functions will be available on initial implementation.
D. Prototyping is being used to confirm that the system meets business requirements.
Correct Answer: B
Explanation: A quality plan is critical to ensure the project's success. Its absence is a major concern because it affects the overall quality and delivery of the system.

Question 501
Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?
A. Intrusion detection systems
B. Data mining techniques
C. Firewalls
D. Packet filtering routers
Correct Answer: B
Explanation: Data mining techniques can analyze patterns and detect anomalies, such as unusual credit card transactions, helping identify possible fraud.

Question 502
Which of the following would BEST help an IS auditor determine whether there is a segregation of duties issue in a critical IT system?
A. Reviewing user access rights
B. Analyzing job roles and responsibilities
C. Examining the IT organization chart
D. Performing a walkthrough of the business processes
Correct Answer: A
Explanation: Reviewing user access rights helps determine whether individuals have conflicting access to critical systems, which can point to segregation of duties issues.

Question 503
During the development of an application, the quality assurance testing and user acceptance testing were combined. The MAJOR concern for an IS auditor reviewing the project is that there will be:
A. Increased maintenance
B. Improper documentation of testing
C. Inadequate functional testing
D. Delays in problem resolution
Correct Answer: C
Explanation:
The major risk of combining quality assurance testing and user acceptance testing is that functional testing may be inadequate. Choices A, B, and D are not as critical.

Question 504
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
Correct Answer: D
Explanation:
The greatest advantage of RAD is the shorter development time frame. Choices A and B are also true but apply to traditional SDLC. Choice C is not necessarily always true.

Question 505
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
Correct Answer: D
Explanation:
Choices A, B, and C are incorrect because they do not pertain to the area being audited. The auditor should ensure that the products to be purchased are compatible with the current or planned OS.

Question 506
The GREATEST benefit in implementing an expert system is the:
A. Capturing of the knowledge and experience of individuals in an organization
B. Sharing of knowledge in a central repository
C. Enhancement of personnel productivity and performance
D. Reduction of employee turnover in key departments
Correct Answer: A
Explanation:
The basis for an expert system is the capture and recording of knowledge and experience. Enhancing productivity is a benefit, but not as critical as knowledge capture.

Question 507
By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:
A. Reliable products are guaranteed
B. Programmers' efficiency is improved
C. Security requirements are designed
D. Predictable software processes are followed

Correct Answer: D

Explanation:

Evaluating against CMM helps determine whether stable, predictable software processes are followed. Mature processes do not guarantee reliability.

Question 508

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

A. Requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate

B. Requirements are well understood and the project is subject to time pressures

C. The project intends to apply an object-oriented design and programming approach

D. The project will involve the use of new technology

Correct Answer: A

Explanation:

The waterfall model is best suited to stable conditions. Iterative development is better for uncertain environments.

Question 509

Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?

A. A sufficient quantity of data for each test case

B. Data representing conditions that are expected in actual processing

C. Completing the test on schedule

D. A random sample of actual data

Correct Answer: B

Explanation:

Selecting the right data is key; it should be representative of actual processing. Quality is more important than quantity.

Question 510

During the review of a web-based software development project, an IS auditor realizes that coding standards are not enforced and code reviews are rarely carried out. This will MOST likely increase the likelihood of a successful:

A. Buffer overflow

B. Brute force attack

C. Distributed denial-of-service attack

D. War dialing attack

Correct Answer: A

Explanation:

Poorly written code is often exploited through buffer overflow techniques. Other options involve different attack vectors.

Question 511

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

A. Bottom up

B. Sociability testing

C. Top-down

D. System test

Correct Answer: C

Explanation:

The top-down approach ensures early detection of interface errors by testing major functions first.

Question 512
During the requirements definition phase of a software development project, the aspects of software testing that should be addressed are developing:
A. Test data covering critical applications
B. Detailed test plans
C. Quality assurance test specifications
D. User acceptance testing specifications
Correct Answer: D
Explanation:
User acceptance test specifications should be developed during the requirements definition phase to ensure the software meets business objectives.

Question 513
Which of the following is an advantage of the top-down approach to software testing?
A. Interface errors are identified early
B. Testing can be started before all programs are complete
C. It is more effective than other testing approaches
D. Errors in critical modules are detected sooner
Correct Answer: A
Explanation:
The top-down approach allows for early testing of major functions, thus detecting interface errors sooner.

Question 514
During the system testing phase of an application development project, the IS auditor should review the:
A. Conceptual design specifications
B. Vendor contract
C. Error reports
D. Program change requests
Correct Answer: C
Explanation:
The IS auditor should review error reports for accuracy in identifying erroneous data and resolution procedures.

Question 515
Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?
A. Increase the time allocated for system testing
B. Implement formal software inspections
C. Increase the development staff
D. Require the sign-off of all project deliverables
Correct Answer: B
Explanation:
Formal software inspections are proven techniques to identify defects early in the development life cycle, reducing correction costs.

Question 516
Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?
A. Applications may not be subject to testing and IT general controls
B. Increased development and maintenance costs
C. Increased application development time
D. Decision-making may be impaired due to diminished responsiveness to requests for information
Correct Answer: A

Explanation:
EUC applications may lack appropriate standards, controls, and quality assurance procedures, posing a significant risk.

Question 517
Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?
A. System owners
B. System users
C. System designers
D. System builders
Correct Answer: A
Explanation:
System owners are responsible for initiating and funding projects, making their involvement crucial from the start.

Question 518
The MAJOR advantage of a component-based development approach is the:
A. Ability to manage an unrestricted variety of data types
B. Provision for modeling complex relationships
C. Capacity to meet the demands of a changing environment
D. Support of multiple development environments
Correct Answer: D
Explanation:
Component-based development allows interaction between different languages and environments, increasing development speed.

Question 519
The specific advantage of white box testing is that it:
A. Verifies a program can operate successfully with other parts of the system
B. Ensures a program's functional operating effectiveness without regard to the internal program structure
C. Determines procedural accuracy or conditions of a program's specific logic paths
D. Examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system
Correct Answer: C
Explanation:
White box testing focuses on assessing the effectiveness of program logic and specific logic paths.

Question 520
Following best practices, formal plans for implementation of new information systems are developed during the:
A. Development phase
B. Design phase
C. Testing phase
D. Deployment phase
Correct Answer: B
Explanation:
Implementation planning should start during the design phase and be revised as development progresses.

Question 521
An IS auditor is reviewing a project that is using an Agile software development approach. Which of the following should the IS auditor expect to find?
A. Use of a process-based maturity model such as the capability maturity model (CMM)
B. Regular monitoring of task-level progress against schedule

C. Extensive use of software development tools to maximize team productivity
D. Post-iteration reviews that identify lessons learned for future use in the project
Correct Answer: D
Explanation:
A key tenet of the Agile approach to software project management is team learning and the use of that learning to refine project management and software development processes as the project progresses. At the end of each iteration, the team considers and documents what worked well and what could have been improved, identifying improvements to implement in subsequent iterations. CMM and Agile operate at opposite ends of the spectrum, as CMM emphasizes predefined formal processes while Agile focuses on adapting processes based on project and team needs.

Question 522
An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?
A. Consider feasibility of a separate user acceptance environment
B. Schedule user testing to occur at a given time each day
C. Implement a source code version control tool
D. Only retest high priority defects
Correct Answer: A
Explanation:
A separate testing environment is necessary for testing to be efficient and effective and to ensure the integrity of production code. This allows defects to be fixed in the development environment without interrupting testing, and also facilitates regression testing when defects are resolved.

Question 523
Which of the following types of testing would determine whether a new or modified system can operate in its target environment without adversely impacting other existing systems?
A. Parallel testing
B. Pilot testing
C. Interface/integration testing
D. Sociability testing
Correct Answer: D
Explanation:
Sociability testing is designed to confirm that a new or modified system can operate in its target environment without adversely affecting existing systems. It encompasses the overall interaction between systems, while the other testing types focus on different aspects of system performance and integration.

Question 524
At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:
A. Report the error as a finding and leave further exploration to the auditee's discretion.
B. Attempt to resolve the error.
C. Recommend that problem resolution be escalated.
D. Ignore the error, as it is not possible to get objective evidence for the software error.
Correct Answer: C
Explanation:
In this situation, it is appropriate for the auditor to escalate the issue to ensure it is addressed. Reporting it as a minor finding or ignoring it would be inadequate since the auditor has a responsibility to ensure that issues are brought to light and resolved appropriately.

Question 525
Which of the following is an implementation risk within the process of decision support systems?

A. Management control
B. Semistructured dimensions
C. Inability to specify purpose and usage patterns
D. Changes in decision processes
Correct Answer: C
Explanation:
The inability to specify purpose and usage patterns poses a significant risk during the implementation of decision support systems (DSS). The other options describe characteristics or challenges associated with DSS but are not direct implementation risks.

Question 526
An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?
A. Pilot
B. Parallel
C. Direct cutover
D. Phased
Correct Answer: C
Explanation:
Direct cutover entails switching to the new system immediately, often without the option to revert to the old system if problems arise. This method carries the highest risk compared to other methods, which allow for gradual transitions and provide opportunities for rollback.

Question 527
Which of the following system and data conversion strategies provides the GREATEST redundancy?
A. Direct cutover
B. Pilot study
C. Phased approach
D. Parallel run
Correct Answer: D
Explanation:
Parallel runs allow both the old and new systems to operate concurrently, providing the greatest redundancy and safety, albeit at higher costs. The other methods do not offer the same level of immediate fallback options.

Question 528
Which of the following would impair the independence of a quality assurance team?
A. Ensuring compliance with development methods
B. Checking the testing assumptions
C. Correcting coding errors during the testing process
D. Checking the code to ensure proper documentation
Correct Answer: C
Explanation:
If the quality assurance team is involved in correcting coding errors, it compromises their independence and violates the segregation of duties principle. The other choices are valid QA functions.

Question 529
From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:
A. A big bang deployment after proof of concept.
B. Prototyping and a one-phase deployment.
C. A deployment plan based on sequenced phases.
D. To simulate the new infrastructure before deployment.
Correct Answer: C

Explanation:
Using a phased approach to implement a large and complex IT infrastructure allows for greater assurance of quality results and minimizes risks. Other methods are riskier due to their sudden implementation nature.

Question 530
An organization is migrating from a legacy system to an enterprise resource planning (ERP) system. While reviewing the data migration activity, the MOST important concern for the IS auditor is to determine that there is a:
A. Correlation of semantic characteristics of the data migrated between the two systems.
B. Correlation of arithmetic characteristics of the data migrated between the two systems.
C. Correlation of functional characteristics of the processes between the two systems.
D. Relative efficiency of the processes between the two systems.
Correct Answer: A
Explanation:
The most critical concern during data migration is ensuring that the semantic meaning of the data is preserved across systems, especially since different systems may represent data differently. Arithmetic and functional characteristics are less significant in this context.

Question 531
The reason a certification and accreditation process is performed on critical systems is to ensure that:
A. Security compliance has been technically evaluated.
B. Data have been encrypted and are ready to be stored.
C. The systems have been tested to run on different platforms.
D. The systems have followed the phases of a waterfall model.
Correct Answer: A
Explanation:
The certification and accreditation process ensures that the security compliance of critical systems has been evaluated. It is not specifically about data encryption or platform compatibility, nor is it tied to a particular software development methodology.

Question 532
An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:
A. EDI trading partner agreements.
B. Physical controls for terminals.
C. Authentication techniques for sending and receiving messages.
D. Program change control procedures.
Correct Answer: C
Explanation:
Authentication techniques for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

Question 533
An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would MOST likely:
A. Check to ensure that the type of transaction is valid for the card type.
B. Verify the format of the number entered then locate it on the database.
C. Ensure that the transaction entered is within the cardholder's credit limit.
D. Confirm that the card is not shown as lost or stolen on the master file.
Correct Answer: B
Explanation:
The initial validation should confirm whether the card is valid. This validity is established through the card number and PIN entered by the user. Based on this initial validation, all other validations will proceed.

Question 534
A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?
A. Key verification.
B. One-for-one checking.
C. Manual recalculations.
D. Functional acknowledgements.
Correct Answer: D
Explanation:
Functional acknowledgements act as an audit trail for EDI transactions and are one of the main controls used in data mapping, ensuring the efficient integration of data in the receiving company.

Question 535
Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would MOST likely focus on a review of:
A. Pre-BPR process flowcharts.
B. Post-BPR process flowcharts.
C. BPR project plans.
D. Continuous improvement and monitoring plans.
Correct Answer: B
Explanation:
An IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process. Reviewing post-BPR process flowcharts provides the necessary insight into the current state of controls.

Question 536
A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:
A. Payroll reports should be compared to input forms.
B. Gross payroll should be recalculated manually.
C. Checks (cheques) should be compared to input forms.
D. Checks (cheques) should be reconciled with output reports.
Correct Answer: A
Explanation:
The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports.

Question 537
Which of the following represents the GREATEST potential risk in an EDI environment?
A. Transaction authorization.
B. Loss or duplication of EDI transmissions.
C. Transmission delay.
D. Deletion or manipulation of transactions prior to or after establishment of application controls.
Correct Answer: A
Explanation:
Since the interaction between parties is electronic, there is no inherent authentication occurring; therefore, transaction authorization is the greatest risk.

Question 538
Which of the following is the MOST critical and contributes the greatest to the quality of data in a data warehouse?
A. Accuracy of the source data.
B. Credibility of the data source.

C. Accuracy of the extraction process.
D. Accuracy of the data transformation.
Correct Answer: A
Explanation:
Accuracy of source data is a prerequisite for the quality of the data in a data warehouse.

Question 539
When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?
A. Use of a cryptographic hashing algorithm.
B. Enciphering the message digest.
C. Deciphering the message digest.
D. A sequence number and time stamp.
Correct Answer: D
Explanation:
A sequence number and/or time stamp built into the message can be checked by the recipient to ensure that the message was not intercepted and replayed, thus preventing duplication.

Question 540
When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:
A. Not be concerned since there may be other compensating controls to mitigate the risks.
B. Ensure that overrides are automatically logged and subject to review.
C. Verify whether all such overrides are referred to senior management for approval.
D. Recommend that overrides not be permitted.
Correct Answer: B
Explanation:
If input procedures allow overrides of data validation and editing, automatic logging should occur, and a management individual who did not initiate the override should review this log.

Question 541
When using an integrated test facility (ITF), an IS auditor should ensure that:
A. Production data are used for testing.
B. Test data are isolated from production data.
C. A test data generator is used.
D. Master files are updated with the test data.
Correct Answer: B
Explanation:
An integrated test facility creates a fictitious file in the database, allowing for test transactions to be processed simultaneously with live data, while ensuring that test data is isolated from production data.

Question 542
A clerk changed the interest rate for a loan on a master file. The rate entered is outside the normal range for such a loan. Which of the following controls is MOST effective in providing reasonable assurance that the change was authorized?
A. The system will not process the change until the clerk's manager confirms the change by entering an approval code.
B. The system generates a weekly report listing all rate exceptions and the report is reviewed by the clerk's manager.
C. The system requires the clerk to enter an approval code.
D. The system displays a warning message to the clerk.
Correct Answer: A

Explanation:
Choice A would prevent or detect the use of an unauthorized interest rate. It ensures that management is involved in the approval process before the change is processed.

Question 543
An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would MOST likely:
A. Check to ensure that the type of transaction is valid for the card type.
B. Verify the format of the number entered then locate it on the database.
C. Ensure that the transaction entered is within the cardholder's credit limit.
D. Confirm that the card is not shown as lost or stolen on the master file.
Correct Answer: B
Explanation:
The initial validation should confirm whether the card is valid. This validity is established through the card number and PIN entered by the user. Based on this initial validation, all other validations will proceed.

Question 544
A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?
A. Key verification.
B. One-for-one checking.
C. Manual recalculations.
D. Functional acknowledgements.
Correct Answer: D
Explanation:
Functional acknowledgements act as an audit trail for EDI transactions and are one of the main controls used in data mapping, ensuring the efficient integration of data in the receiving company.

Question 545
Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would MOST likely focus on a review of:
A. Pre-BPR process flowcharts.
B. Post-BPR process flowcharts.
C. BPR project plans.
D. Continuous improvement and monitoring plans.
Correct Answer: B
Explanation:
An IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process. Reviewing post-BPR process flowcharts provides the necessary insight into the current state of controls.

Question 546
A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:
A. Payroll reports should be compared to input forms.
B. Gross payroll should be recalculated manually.
C. Checks (cheques) should be compared to input forms.
D. Checks (cheques) should be reconciled with output reports.
Correct Answer: A
Explanation:
The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports.

Question 547

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

A. Transaction authorization.

B. Loss or duplication of EDI transmissions.

C. Transmission delay.

D. Deletion or manipulation of transactions prior to or after establishment of application controls.

Correct Answer: A

Explanation:

Since the interaction between parties is electronic, there is no inherent authentication occurring; therefore, transaction authorization is the greatest risk.

Question 548

Which of the following is the MOST critical and contributes the greatest to the quality of data in a data warehouse?

A. Accuracy of the source data.

B. Credibility of the data source.

C. Accuracy of the extraction process.

D. Accuracy of the data transformation.

Correct Answer: A

Explanation:

Accuracy of source data is a prerequisite for the quality of the data in a data warehouse.

Question 549

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

A. Use of a cryptographic hashing algorithm.

B. Enciphering the message digest.

C. Deciphering the message digest.

D. A sequence number and time stamp.

Correct Answer: D

Explanation:

A sequence number and/or time stamp built into the message can be checked by the recipient to ensure that the message was not intercepted and replayed, thus preventing duplication.

Question 550

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

A. Not be concerned since there may be other compensating controls to mitigate the risks.

B. Ensure that overrides are automatically logged and subject to review.

C. Verify whether all such overrides are referred to senior management for approval.

D. Recommend that overrides not be permitted.

Correct Answer: B

Explanation:

If input procedures allow overrides of data validation and editing, automatic logging should occur, and a management individual who did not initiate the override should review this log.

Question 551

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

A. Production data are used for testing.

B. Test data are isolated from production data.

C. A test data generator is used.

D. Master files are updated with the test data.

Correct Answer: B

Explanation:
An integrated test facility creates a fictitious file in the database, allowing for test transactions to be processed simultaneously with live data, while ensuring that test data is isolated from production data.

Question 552
A clerk changed the interest rate for a loan on a master file. The rate entered is outside the normal range for such a loan. Which of the following controls is MOST effective in providing reasonable assurance that the change was authorized?
A. The system will not process the change until the clerk's manager confirms the change by entering an approval code.
B. The system generates a weekly report listing all rate exceptions and the report is reviewed by the clerk's manager.
C. The system requires the clerk to enter an approval code.
D. The system displays a warning message to the clerk.
Correct Answer: A
Explanation:
Choice A would prevent or detect the use of an unauthorized interest rate. It ensures that management is involved in the approval process before the change is processed.

Question 553
The GREATEST advantage of using web services for the exchange of information between two systems is:
A. secure communications.
B. improved performance.
C. efficient interfacing.
D. enhanced documentation.
Correct Answer: C
Explanation:
Web services facilitate the exchange of information between two systems, regardless of the operating system or programming language used. Communication is not necessarily securer or faster, and there is no documentation benefit in using web services.

Question 554
An IS auditor reviewing an accounts payable system discovers that audit logs are not being reviewed. When this issue is raised with management the response is that additional controls are not necessary because effective system access controls are in place. The BEST response the auditor can make is to:
A. review the integrity of system access controls.
B. accept management's statement that effective access controls are in place.
C. stress the importance of having a system control framework in place.
D. review the background checks of the accounts payable staff.
Correct Answer: C
Explanation:
Experience has demonstrated that reliance purely on preventative controls is dangerous. Preventative controls may not prove to be as strong as anticipated or their effectiveness can deteriorate over time. Evaluating the cost of controls versus the quantum of risk is a valid management concern. However, in a high-risk system, a comprehensive control framework is needed, intelligent design should permit additional detective and corrective controls to be established that don't have high ongoing costs, e.g., automated interrogation of logs to highlight suspicious individual transactions or data patterns. Effective access controls are, in themselves, a positive but, for reasons outlined above, may not sufficiently compensate for other control weaknesses. In this situation, the IS auditor needs to be proactive. The IS auditor has a fundamental obligation to point out control weaknesses that give rise to unacceptable risks to the organization and work with management to have these corrected. Reviewing background checks on accounts payable staff does not provide evidence that fraud will not occur.

Question 555

When evaluating the controls of an EDI application, an IS auditor should PRIMARILY be concerned with the risk of:

A. excessive transaction turnaround time.

B. application interface failure.

C. improper transaction authorization.

D. nonvalidated batch totals.

Correct Answer: C

Explanation:

Foremost among the risks associated with electronic data interchange (EDI) is improper transaction authorization. Since the interaction with the parties is electronic, there is no inherent authentication. The other choices, although risks, are not as significant.

Question 556

When reviewing an organization's approved software product list, which of the following is the MOST important thing to verify?

A. The risks associated with the use of the products are periodically assessed.

B. The latest version of software is listed for each product.

C. Due to licensing issues, the list does not contain open source software.

D. After hours support is offered.

Correct Answer: A

Explanation:

Since the business conditions surrounding vendors may change, it is important for an organization to conduct periodic risk assessments of the vendor software list. This might be best incorporated into the IT risk management process. Choices B, C, and D are possible considerations but would not be the most important.

Question 557

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

A. reverse engineering.

B. prototyping.

C. software reuse.

D. reengineering.

Correct Answer: D

Explanation:

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

Question 558

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

A. Unit testing

B. Integration testing

C. Design walkthroughs

D. Configuration management

Correct Answer: B

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

Question 559
An IS auditor performing an application maintenance audit would review the log of program changes for the:
A. authorization of program changes.
B. creation date of a current object module.
C. number of program changes actually made.
D. creation date of a current source program.
Correct Answer: A
Explanation:
The manual log will most likely contain information on authorized changes to a program. Deliberate, unauthorized changes will not be documented by the responsible party. An automated log, found usually in library management products, and not a changelog would most likely contain date information for the source and executable modules.

Question 560
After discovering a security vulnerability in a third-party application that interfaces with several external systems, a patch is applied to a significant number of modules. Which of the following tests should an IS auditor recommend?
A. Stress
B. Black box
C. Interface
D. System
Correct Answer: D
Explanation:
Given the extensiveness of the patch and its interfaces to external systems, system testing is most appropriate. Interface testing is not enough, and stress or black box testing are inadequate in these circumstances.

Question 561
When performing an audit of a client relationship management (CRM) system migration project, which of the following should be of GREATEST concern to an IS auditor?
A. The technical migration is planned for a Friday preceding a long weekend, and the time window is too short for completing all tasks.
B. Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old system.
C. A single implementation is planned, immediately decommissioning the legacy system.
D. Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's software.
Correct Answer: C
Explanation:
Major system migrations should include a phase of parallel operation or a phased cut-over to reduce implementation risks. Decommissioning or disposing of the old hardware would complicate any fallback strategy should the new system not operate correctly. A weekend can be used as a time buffer so that the new system will have a better chance of being up and running after the weekend. A different data representation does not mean different data presentation at the front end. Even when this is the case, this issue can be solved by adequate training and user support. The printing functionality is commonly one of the last functions to be tested in a new system because it is usually the last step performed in any business event. Thus, meaningful testing and the respective error fixing are only possible after all other parts of the software have been successfully tested.

Question 562

Which of the following reports should an IS auditor use to check compliance with a service level agreement's (SLA) requirement for uptime?
A. Utilization reports
B. Hardware error reports
C. System logs
D. Availability reports
Correct Answer: D
Explanation:
IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. System logs are a recording of the system's activities.

Question 563
A benefit of quality of service (QoS) is that the:
A. entire network's availability and performance will be significantly improved.
B. telecom carrier will provide the company with accurate service-level compliance reports.
C. participating applications will have guaranteed service levels.
D. communications link will be supported by security controls to perform secure online transactions.
Correct Answer: C
Explanation:
The main function of QoS is to optimize network performance by assigning priority to business applications and end users through the allocation of dedicated parts of the bandwidth to specific traffic. Choice A is not true because the communication itself will not be improved. While the speed of data exchange for specific applications could be faster, availability will not be improved. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service-level reports. Even when QoS is integrated with firewalls, VPNs, encryption tools, and others, the tool itself is not intended to provide security controls.

Question 564
An organization has outsourced its help desk. Which of the following indicators would be the best to include in the SLA?
A. Overall number of users supported
B. Percentage of incidents solved in the first call
C. Number of incidents reported to the help desk
D. Number of agents answering the phones
Correct Answer: B
Explanation:
Since it is about service level (performance) indicators, the percentage of incidents solved on the first call is the only option that is relevant. Choices A, C, and D are not quality measures of the help desk service.

Question 565
The PRIMARY objective of service-level management (SLM) is to:
A. define, agree, record, and manage the required levels of service.
B. ensure that services are managed to deliver the highest achievable level of availability.
C. keep the costs associated with any service at a minimum.
D. monitor and report any legal noncompliance to business management.
Correct Answer: A
Explanation:
The objective of service-level management (SLM) is to negotiate, document, and manage (i.e., provide and monitor) the services in the manner in which the customer requires those services. This does not necessarily ensure that services are delivered at the highest achievable level of availability (e.g., redundancy and clustering).

Although maximizing availability might be necessary for some critical services, it cannot be applied as a general rule of thumb. SLM cannot ensure that costs for all services will be kept at a low or minimum level since costs associated with a service will directly reflect the customer's requirements. Monitoring and reporting legal noncompliance is not a part of SLM.

Question 566

Which of the following should be of PRIMARY concern to an IS auditor reviewing the management of external IT service providers?

A. Minimizing costs for the services provided

B. Prohibiting the provider from subcontracting services

C. Evaluating the process for transferring knowledge to the IT department

D. Determining if the services were provided as contracted

Correct Answer: D

Explanation:

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

Question 567

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

A. minimize costs associated with disaster-resilient components.

B. provide for sufficient capacity to meet the agreed-upon demands of the business.

C. provide reasonable assurance that agreed-upon obligations to customers can be met.

D. produce timely performance metric reports.

Correct Answer: C

Explanation:

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

Question 568

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

A. Postpone the audit until the agreement is documented

B. Report the existence of the undocumented agreement to senior management

C. Confirm the content of the agreement with both departments

D. Draft a service level agreement (SLA) for the two departments

Correct Answer: C

Explanation:

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

Question 569

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

A. The use of diskless workstations

B. Periodic checking of hard drives

C. The use of current antivirus software

D. Policies that result in instant dismissal if violated

Correct Answer: B

Explanation:

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

Question 570

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

A. System access log files

B. Enabled access control software parameters

C. Logs of access control violations

D. System configuration files for control options used

Correct Answer: D

Explanation:

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

Question 571

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

A. A system downtime log

B. Vendors' reliability figures

C. Regularly scheduled maintenance log

D. A written preventive maintenance schedule

Correct Answer: A

Explanation:

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

Question 572

Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?

A. Sensitive data can be read by operators.

B. Data can be amended without authorization.

C. Unauthorized report copies can be printed.

D. Output can be lost in the event of system failure.

Correct Answer: C

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

Question 573
Applying a retention date on a file will ensure that:
A. data cannot be read until the date is set.
B. data will not be deleted before that date.
C. backup copies are not retained after that date.
D. datasets having the same name are differentiated.
Correct Answer: B
Explanation:
A retention date will ensure that a file cannot be overwritten before that date has passed. The retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and therefore may be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

Question 574
Which of the following is a network diagnostic tool that monitors and records network information?
A. Online monitor
B. Downtime report
C. Help desk report
D. Protocol analyzer
Correct Answer: D
Explanation:
Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached. Online monitors measure telecommunications transmissions and determine whether transmissions were accurate and complete. Downtime reports track the availability of telecommunication lines and circuits. Help desk reports are prepared by the help desk, which is staffed or supported by IS technical support personnel trained to handle problems occurring during the course of IS operations.

Question 575
Which of the following will help detect changes made by an intruder to the system log of a server?
A. Mirroring the system log on another server
B. Simultaneously duplicating the system log on a write-once disk
C. Write-protecting the directory containing the system log
D. Storing the backup of the system log offsite
Correct Answer: B
Explanation:
A write-once CD cannot be overwritten. Therefore, the system log duplicated on the disk could be compared to the original log to detect differences, which could be the result of changes made by an intruder. Write-protecting the system log does not prevent deletion or modification, since the superuser can override the write protection. Backup and mirroring may overwrite earlier files and may not be current.

Question 576
IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?
A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.
B. The service provider does not have incident handling procedures.
C. Recently a corrupted database could not be recovered because of library management problems.

D. Incident logs are not being reviewed.

Correct Answer: A

Explanation:

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

Question 577

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

A. Protecting the server in a secure location

B. Setting a boot password

C. Hardening the server configuration

D. Implementing activity logging

Correct Answer: C

Explanation:

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

Question 578

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

A. contents are highly volatile.

B. data cannot be backed up.

C. data can be copied.

D. device may not be compatible with other peripherals.

Correct Answer: C

Explanation:

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

Question 579

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

A. loss of confidentiality.

B. increased redundancy.

C. unauthorized accesses.

D. application malfunctions.

Correct Answer: B

Explanation:

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

Question 580

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

A. protect the organization from viruses and nonbusiness materials.

B. maximize employee performance.

C. safeguard the organization's image.

D. assist the organization in preventing legal issues.

Correct Answer: A

Explanation:

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

QUESTION 581

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

- Compression software to minimize transmission duration.
- Functional or message acknowledgments.
- A packet-filtering firewall to reroute messages.
- Leased asynchronous transfer mode lines.

Correct Answer: D

Section: IT SERVICE DELIVERY AND SUPPORT

Explanation:

Leased asynchronous transfer mode lines avoid using public and shared infrastructures that have a greater number of communication failures. Compression software reduces transmission time but is not as effective as leased lines. Functional acknowledgments help if communication lines introduce noise but don’t assist if a link is down. A packet-filtering firewall does not reroute messages.

QUESTION 582

An IS auditor reviewing an organization's data file control procedures finds that transactions are applied to the most current files, while restart procedures use earlier versions. The IS auditor should recommend the implementation of:

- Source documentation retention.
- Data file security.
- Version usage control.
- One-for-one checking.

Correct Answer: C

Section: IT SERVICE DELIVERY AND SUPPORT

Explanation:

Proper version usage is essential to ensure that the correct database version is used for transactions and restarts. Source documentation retention helps with verification but does not ensure the use of the correct file. Data file security prevents unauthorized access but does not address versioning. One-for-one checking ensures that all documents are processed but does not ensure the correct version is used.

QUESTION 583

Which of the following BEST limits the impact of server failures in a distributed environment?

- Redundant pathways
- Clustering
- Dial backup lines
- Standby power

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Clustering allows multiple servers to operate as a unit, ensuring that when one fails, another can take over. Redundant pathways and dial backup lines are designed for communication failures, not server failures. Standby power provides an alternative power source but does not address server failures.

QUESTION 584
When reviewing a hardware maintenance program, an IS auditor should assess whether:

- The schedule of all unplanned maintenance is maintained.
- It is in line with historical trends.
- It has been approved by the IS steering committee.
- The program is validated against vendor specifications.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The maintenance program should be validated against vendor specifications to ensure it meets the hardware's operational needs. Unplanned maintenance cannot be scheduled, and maintenance programs do not require approval by the steering committee or alignment with historical trends.

QUESTION 585
An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the MOST effective compensating control for this weakness?

- Staging and job setup
- Supervisory review of logs
- Regular back-up of tapes
- Offsite storage of tapes

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Effective staging and job setup can act as a compensating control for the weakness found in tape management. Supervisory review is a detective control, while regular backups and offsite storage are corrective controls that do not directly address the bypass of tape header records.

QUESTION 586
To verify that the correct version of a data file was used for a production run, an IS auditor should review:

- Operator problem reports.
- Operator work schedules.
- System logs.
- Output distribution reports.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
System logs provide automated reports identifying activities performed on the computer, allowing the auditor to verify the correct file version was used. Operator problem reports and work schedules do not assist in this verification, and output distribution reports focus on report generation rather than file version usage.

QUESTION 587
Which of the following is the BEST type of program for an organization to implement to aggregate, correlate, and store different log and event files, and then produce weekly and monthly reports for IS auditors?

- A security information event management (SIEM) product

- An open-source correlation engine
- A log management tool
- An extract, transform, load (ETL) system

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
A log management tool is specifically designed for aggregating and storing log events from various sources and producing reports, making it the best choice. A SIEM product has similar features but is not primarily focused on long-term storage and reporting of logs. An open-source correlation engine is a part of a SIEM, while an ETL system is unrelated to log management.

QUESTION 588
Doing which of the following during peak production hours could result in unexpected downtime?

- Performing data migration or tape backup
- Performing preventive maintenance on electrical systems
- Promoting applications from development to the staging environment
- Replacing a failed power supply in the core router of the data center

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Preventive maintenance activities should ideally be scheduled during non-peak times. Performing such maintenance during peak hours could inadvertently lead to unplanned downtime, whereas the other options generally do not cause downtime.

QUESTION 589
Which of the following would BEST maintain the integrity of a firewall log?

- Granting access to log information only to administrators
- Capturing log events in the operating system layer
- Writing dual logs onto separate storage media
- Sending log information to a dedicated third-party log server

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Establishing a dedicated third-party log server enhances log integrity by reducing the risk of unauthorized modifications. Limited access to log information primarily supports confidentiality rather than integrity. Capturing logs in the operating system layer does not enhance integrity, and dual logs mainly ensure availability rather than integrity.

QUESTION 590
Which of the following will prevent dangling tuples in a database?

- Cyclic integrity
- Domain integrity
- Relational integrity
- Referential integrity

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Referential integrity ensures that all foreign keys in a table have corresponding primary keys in another table, thus preventing dangling tuples. Cyclic integrity is not a recognized term, domain integrity relates to data value ranges, and relational integrity pertains to record-level validation.

QUESTION 591

The objective of concurrency control in a database system is to:

- Restrict updating of the database to authorized users.
- Prevent integrity problems when two processes attempt to update the same data at the same time.
- Prevent inadvertent or unauthorized disclosure of data in the database.
- Ensure the accuracy, completeness, and consistency of data.

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Concurrency controls are designed to prevent data integrity issues when multiple processes try to access the same data simultaneously. The other options relate to access controls and data quality but do not specifically address concurrency.

QUESTION 592
Which of the following controls would provide the GREATEST assurance of database integrity?

- Audit log procedures
- Table link/reference checks
- Query/table access time checks
- Rollback and rollforward database features

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Table link/reference checks detect linking errors and ensure completeness and accuracy of database contents, providing the highest assurance of integrity. Audit logs help trace events but do not ensure database content integrity. Query checks improve performance, and rollback features focus on transaction recovery rather than overall database integrity.

QUESTION 593
An IS auditor analyzing the audit log of a database management system (DBMS) finds that some transactions were partially executed as a result of an error, and are not rolled back. Which of the following transaction processing features has been violated?

- Consistency
- Isolation
- Durability
- Atomicity

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Atomicity ensures that transactions are fully processed or not at all. If a transaction is partially executed without rollback, atomicity is violated. Consistency ensures legal database states, isolation keeps transactions invisible to each other during processing, and durability ensures completed transactions persist.

QUESTION 594
During maintenance of a relational database, several values of the foreign key in a transaction table of a relational database have been corrupted. The consequence is that:

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

Correct Answer: A

Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Corruption of foreign keys prevents the application from correctly associating master data with transaction data, which can lead to processing errors. The other options incorrectly suggest immediate or severe consequences from foreign key corruption.

QUESTION 595
In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

- Foreign key
- Primary key
- Secondary key
- Public key

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Foreign keys enforce referential integrity, preventing deletions that would result in orphaned records in related tables. Primary keys identify records within a single table, while secondary and public keys do not enforce referential relationships.

QUESTION 596
Which of the following types of controls would MOST likely ensure the reliability of a network in an organization?

- Physical controls
- Management controls
- Operational controls
- Technical controls

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Technical controls, such as firewalls, intrusion detection systems, and encryption, are essential for ensuring the reliability and security of a network. Physical controls focus on protecting hardware, while management and operational controls relate to policies and procedures but do not directly ensure network reliability.

QUESTION 597
An organization wants to ensure that its database transactions are processed accurately and reliably. Which of the following is the MOST appropriate method to achieve this?

- Implementing a high-availability configuration
- Using transaction logging
- Performing regular backups
- Applying encryption techniques

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Transaction logging captures all changes made to the database, enabling accurate recovery and rollback in case of errors, thus ensuring the reliability of transactions. High-availability configurations improve uptime but do not address transaction accuracy. Backups are important but do not ensure transaction reliability in real-time, and encryption protects data confidentiality rather than transaction accuracy.

QUESTION 598

Which of the following BEST describes the purpose of a change management process in IT?

- To minimize the risk of downtime during system upgrades.
- To document all technical specifications for future reference.
- To control and manage changes to IT systems and infrastructure.
- To ensure compliance with regulatory requirements.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The primary purpose of change management is to control and manage changes to IT systems and infrastructure to minimize disruption and maintain system integrity. While minimizing downtime and ensuring compliance are important, they are not the main focus of change management.

QUESTION 599
When evaluating the effectiveness of a disaster recovery plan, an IS auditor should FIRST verify that:

- Backup procedures are documented and updated regularly.
- Business impact analyses have been performed.
- Recovery time objectives (RTO) are clearly defined.
- The plan is tested and the results documented.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Testing the disaster recovery plan and documenting the results is essential to ensure that it works as intended. While the other options are important, the effectiveness of a plan is primarily demonstrated through testing.

QUESTION 600
An organization is planning to implement a new information system. The MOST important factor to consider during the system's design phase is:

- Integration with existing systems.
- Compliance with regulatory requirements.
- User training and support.
- Data migration strategies.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Integration with existing systems is crucial to ensure the new system operates effectively within the organization's IT environment. Compliance, training, and data migration are also important but secondary to ensuring seamless integration.

QUESTION 601
Which of the following is widely accepted as one of the critical components in networking management?

- Configuration management
- Topological mappings
- Application of monitoring tools
- Proxy server troubleshooting

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Configuration management is widely accepted as a key component in networking management. It deals with maintaining the network's structure, ensuring functionality, and monitoring performance. While topological mappings provide outlines of network connectivity, application monitoring and proxy server troubleshooting are not as integral to overall network management.

QUESTION 602
Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?

- Parity check
- Echo check
- Block sum check
- Cyclic redundancy check

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Cyclic redundancy check (CRC) is highly effective for detecting errors in network transmissions. CRC verifies blocks of data and can detect multiple errors within a transmission. Parity and echo checks are less effective for detecting bursts of errors.

QUESTION 603
Which of the following types of firewalls provide the GREATEST degree and granularity of control?

- Screening router
- Packet filter
- Application gateway
- Circuit gateway

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Application gateways offer the highest degree of control and granularity by inspecting the payload of packets, allowing for more detailed security decisions. In contrast, screening routers and packet filters operate primarily at the network layer, and circuit gateways establish connections but do not inspect content at the same level.

QUESTION 604
Which of the following is MOST directly affected by network performance monitoring tools?

- Integrity
- Availability
- Completeness
- Confidentiality

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Network performance monitoring tools are primarily concerned with availability, ensuring that the network remains operational. These tools help detect service disruptions but do not directly address data integrity, completeness, or confidentiality.

QUESTION 605
A review of wide area network (WAN) usage discovers that traffic on one communication line between sites, synchronously linking the master and standby database, peaks at 96 percent of the line capacity. An IS auditor should conclude that:

- Analysis is required to determine if a pattern emerges that results in a service loss for a short period of time.
- WAN capacity is adequate for the maximum traffic demands since saturation has not been reached.
- The line should immediately be replaced by one with a larger capacity to provide approximately 85 percent saturation.
- Users should be instructed to reduce their traffic demands or distribute them across all service hours to flatten bandwidth consumption.

Correct Answer: A

Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Before recommending upgrades, the IS auditor should conduct an analysis to determine if high usage is consistent or an anomaly. If it is a regular occurrence, more capacity may be required. Occasional peaks do not justify immediate line replacement.

QUESTION 606
While reviewing the IT infrastructure, an IS auditor notices that storage resources are continuously being added. The IS auditor should:

- Recommend the use of disk mirroring.
- Review the adequacy of offsite storage.
- Review the capacity management process.
- Recommend the use of a compression algorithm.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The IS auditor should focus on reviewing the capacity management process to ensure that resources are being used efficiently. This will help anticipate future needs and prevent overspending or resource shortages. Disk mirroring and compression may address storage issues but are not the primary focus in this scenario.

QUESTION 607
In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

- Automated logging of changes to development libraries
- Additional staff to provide separation of duties
- Procedures that verify that only approved program changes are implemented
- Access controls to prevent the operator from making program modifications

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
In small organizations where segregation of duties may not be possible, compensating controls should be implemented. Verifying that only approved changes are made ensures accountability and security. While additional staff would be ideal, it may not be feasible.

QUESTION 608
Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?

- Assess the impact of patches prior to installation.
- Ask the vendors for a new software version with all fixes included.
- Install the security patch immediately.
- Decline to deal with these vendors in the future.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Before applying any patch, it is important to assess its impact on existing systems to avoid disrupting other functionalities. Installing patches immediately without proper testing could introduce new issues. Seeking a full software version or avoiding the vendor is not practical in most cases.

QUESTION 609
Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?

- Release-to-release source and object comparison reports

- Library control software restricting changes to source code
- Restricted access to source code and object code
- Date and time-stamp reviews of source and object code

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Date and time-stamp reviews ensure that the source and object code are synchronized after compilation. This is the most reliable way to verify that the production object code matches the approved source code.

QUESTION 610
Change management procedures are established by IS management to:

- Control the movement of applications from the test environment to the production environment.
- Control the interruption of business operations from lack of attention to unresolved problems.
- Ensure the uninterrupted operation of the business in the event of a disaster.
- Verify that system changes are properly documented.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Change management procedures are primarily established to control the migration of applications from the test to production environment. They ensure that only tested and approved applications are deployed, minimizing risks to business operations.

QUESTION 611
In regard to moving an application program from the test environment to the production environment, the BEST control would be to have the:

- Application programmer copy the source program and compiled object module to the production libraries.
- Application programmer copy the source program to the production libraries and then have the production control group compile the program.
- Production control group compile the object module to the production libraries using the source program in the test environment.
- Production control group copy the source program to the production libraries and then compile the program.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The best control involves having the production control group copy the source program to the production libraries and compile it. This reduces the risk of unauthorized changes being introduced into the production environment.

QUESTION 612
An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered an adequate set of compensating controls?

- Allow changes to be made only with the DBA user account.
- Make changes to the database after granting access to a normal user account.
- Use the DBA user account to make changes, log the changes, and review the change log the following day.
- Use the normal user account to make changes, log the changes, and review the change log the following day.

Correct Answer: C

Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Using the DBA account for changes, logging the changes, and reviewing the log the next day is an effective compensating control. It allows monitoring of changes made outside of normal hours, reducing the risk of unauthorized modifications.

QUESTION 613
Which of the following tests performed by an IS auditor would be the MOST effective in determining compliance with an organization's change control procedures?

- Review software migration records and verify approvals.
- Identify changes that have occurred and verify approvals.
- Review change control documentation and verify approvals.
- Ensure that only appropriate staff can migrate changes into production.

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Identifying actual changes and verifying their approvals is the most effective way to determine compliance with change control procedures. This method checks what has occurred, as opposed to only reviewing records or documentation.

QUESTION 614
An IS auditor reviewing a database application discovers that the current configuration does not match the originally designed structure. Which of the following should be the IS auditor's next action?

- Analyze the need for the structural change.
- Recommend restoration to the originally designed structure.
- Recommend the implementation of a change control process.
- Determine if the modifications were properly approved.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The IS auditor's next step should be to determine if the modifications were properly approved. This ensures that any changes to the database configuration were authorized, preventing unauthorized alterations.

QUESTION 615
A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST effectively detect the malicious activity?

- Comparing source code
- Reviewing system log files
- Comparing object code
- Reviewing executable and source code integrity

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Reviewing system log files is the best method to detect malicious activity, as they provide a record of actions performed in the system. Comparing code is ineffective if the original code is restored, and integrity checks wouldn't reveal past malicious actions.

QUESTION 616
The purpose of code signing is to provide assurance that:

- The software has not been subsequently modified.

- The application can safely interface with another signed application.
- The signer of the application is trusted.
- The private key of the signer has not been compromised.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Code signing ensures that the executable code has not been modified after being signed. The other options describe potential weaknesses of code signing or other security concerns unrelated to its primary purpose.

QUESTION 617
An IS auditor should recommend the use of library control software to provide reasonable assurance that:

- Program changes have been authorized.
- Only thoroughly tested programs are released.
- Modified programs are automatically moved to production.
- Source and executable code integrity is maintained.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Library control software is primarily used to ensure that program changes are authorized before they are moved to production. While it can provide assurance for some aspects of source and executable code integrity, its main function is controlling changes.

QUESTION 618
An organization has recently installed a security patch, which crashed the production server. To minimize the probability of this occurring again, an IS auditor should:

- Apply the patch according to the patch's release notes.
- Ensure that a good change management process is in place.
- Thoroughly test the patch before sending it to production.
- Approve the patch after doing a risk assessment.

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The IS auditor should focus on ensuring that a good change management process is in place, which includes proper testing and risk assessment of patches. Testing patches before production is a part of this overall process, but the change management process is key to preventing future issues.

QUESTION 619
When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

- Allow changes, which will be completed using after-the-fact follow-up.
- Allow undocumented changes directly to the production library.
- Do not allow any emergency changes.
- Allow programmers permanent access to production programs.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Emergency changes should be allowed but completed with after-the-fact follow-up to ensure proper documentation and review. This allows for quick fixes while maintaining control over production environments.

QUESTION 620
To determine if unauthorized changes have been made to production code the BEST audit procedure is to:

- Examine the change control system records and trace them forward to object code files.

- Review access control permissions operating within the production program libraries.
- Examine object code to find instances of changes and trace them back to change control records.
- Review change approved designations established within the change control system.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Examining object code to identify changes and tracing them back to change control records is the best way to determine if unauthorized changes have been made. This provides a direct check of the actual production environment.

QUESTION 621
The application systems of an organization using open-source software have no single recognized developer producing patches. Which of the following would be the MOST secure way of updating open-source software?

- Rewrite the patches and apply them.
- Code review and application of available patches.
- Develop in-house patches.
- Identify and test suitable patches before applying them.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The most secure approach is to identify and test suitable patches before applying them. This reduces the risk of applying faulty or malicious patches.

QUESTION 622
An IS auditor discovers that developers have operator access to the command line of a production environment operating system. Which of the following controls would BEST mitigate the risk of undetected and unauthorized program changes to the production environment?

- Commands typed on the command line are logged.
- Hash keys are calculated periodically for programs and matched against hash keys calculated for the most recent authorized versions of the programs.
- Access to the operating system command line is granted through an access restriction tool with preapproved rights.
- Software development tools and compilers have been removed from the production environment.

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Periodic calculation of hash keys for programs and matching them against the most recent authorized versions ensures the detection of unauthorized changes. Logs and access restriction tools can help, but they don't directly address unauthorized changes.

QUESTION 623
Which of the following processes should an IS auditor recommend to assist in the recording of baselines for software releases?

- Change management.
- Backup and recovery.
- Incident management.
- Configuration management.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Configuration management includes tools and processes for recording baselines of software releases. These baselines can be used as a point of reference if issues arise in future releases.

QUESTION 624

An IS auditor notes that patches for the operating system used by an organization are deployed by the IT department as advised by the vendor. The MOST significant concern an IS auditor should have with this practice is the nonconsideration by IT of:

- The training needs for users after applying the patch.
- Any beneficial impact of the patch on the operational systems.
- Delaying deployment until testing the impact of the patch.
- The necessity of advising end users of new patches.

Correct Answer: C

Section: IT SERVICE DELIVERY AND SUPPORT

Explanation:

The most significant concern is the lack of testing. Applying patches without testing risks system disruption. Training users or advising them of patches is less critical than preventing system outages.

QUESTION 625

In a small organization, developers may release emergency changes directly to production. Which of the following will BEST control the risk in this situation?

- Approve and document the change the next business day.
- Limit developer access to production to a specific timeframe.
- Obtain secondary approval before releasing to production.
- Disable the compiler option in the production machine.

Correct Answer: A

Section: IT SERVICE DELIVERY AND SUPPORT

Explanation:

In emergency situations, allowing developers to release changes directly can be acceptable as long as the change is documented and approved retroactively. Limiting access to timeframes or requiring secondary approval can hinder timely fixes.

QUESTION 626

Time constraints and expanded needs have been found by an IS auditor to be the root causes for recent violations of corporate data definition standards in a new business intelligence project. Which of the following is the MOST appropriate suggestion for an auditor to make?

- Achieve standards alignment through an increase of resources devoted to the project.
- Align the data definition standards after completion of the project.
- Delay the project until compliance with standards can be achieved.
- Enforce standard compliance by adopting punitive measures against violators.

Correct Answer: A

Section: IT SERVICE DELIVERY AND SUPPORT

Explanation:

The best suggestion is to increase resources to ensure compliance with standards. Delaying the project or enforcing punitive measures could impact project success, while aligning standards post-project poses risks to consistency and quality.

QUESTION 627

After installing a network, an organization installed a vulnerability assessment tool or security scanner to identify possible weaknesses. Which is the MOST serious risk associated with such tools?

- Differential reporting.
- False-positive reporting.
- False-negative reporting.
- Less-detail reporting.

Correct Answer: C

Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
False-negative reporting is the most serious risk because it means vulnerabilities could go undetected and unaddressed. While false positives are also a concern, they at least prompt further investigation, whereas false negatives leave the system exposed.

QUESTION 628
The FIRST step in managing the risk of a cyber attack is to:

- Assess the vulnerability impact.
- Evaluate the likelihood of threats.
- Identify critical information assets.
- Estimate potential damage.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The first step in managing risk is identifying and classifying critical information assets. This allows for prioritization of protective measures based on the value and sensitivity of these assets. Threat evaluation and impact assessment follow this step.

QUESTION 629
Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits a vulnerability in a protocol?

- Install the vendor's security fix for the vulnerability.
- Block the protocol traffic in the perimeter firewall.
- Block the protocol traffic between internal network segments.
- Stop the service until an appropriate security fix is installed.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Stopping the vulnerable service and then applying the appropriate security fix is the most effective method to prevent a network worm from spreading. Simply blocking traffic or installing fixes while the service is still running may not fully stop the worm's propagation.

QUESTION 630
The PRIMARY objective of performing a post-incident review is that it presents an opportunity to:

- Improve internal control procedures.
- Harden the network to industry best practices.
- Highlight the importance of incident response management to management.
- Improve employee awareness of the incident response process.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The main goal of a post-incident review is to improve internal control procedures by learning from the incident. This process helps to prevent future incidents and strengthen the organization's overall security posture.

QUESTION 631
The computer security incident response team (CSIRT) of an organization disseminates detailed descriptions of recent threats. An IS auditor's GREATEST concern should be that the users might:

- Use this information to launch attacks.
- Forward the security alert.
- Implement individual solutions.

- Fail to understand the threat.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
An organization's CSIRT should disseminate recent threats to assist users in understanding security risks. However, this poses the risk that users might misuse the information to launch attacks. Forwarding alerts is generally harmless, implementing individual solutions is unlikely to happen, and failing to understand the threat is not as critical a concern.

QUESTION 632
The MAIN criterion for determining the severity level of a service disruption incident is:

- Cost of recovery.
- Negative public opinion.
- Geographic location.
- Downtime.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The longer the downtime, the greater the severity of the incident. Cost of recovery may be minimal, yet downtime can have a significant impact. Negative public opinion is a symptom, and geographic location does not affect severity.

QUESTION 633
Which of the following would be an indicator of the effectiveness of a computer security incident response team?

- Financial impact per security incident.
- Number of security vulnerabilities that were patched.
- Percentage of business applications that are being protected.
- Number of successful penetration tests.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The financial impact per security incident is the most important indicator of effectiveness. While the other options measure aspects of security, they do not directly indicate the response team's effectiveness.

QUESTION 634
An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if:

- The setup is geographically dispersed.
- The network servers are clustered in a site.
- A hot site is ready for activation.
- Diverse routing is implemented for the network.

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Clustering servers in one location poses a risk to the entire network if that site experiences a disaster, creating a single point of failure. Geographical dispersion and diverse routing provide alternative options.

QUESTION 635
Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

- Firewalls
- Routers
- Layer 2 switches

- VLANs

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Firewalls are the primary tools to prevent unauthorized access between network segments, while routers and switches have different functionalities regarding packet handling and traffic segregation.

QUESTION 636
A company is implementing a dynamic host configuration protocol (DHCP). Given that the following conditions exist, which represents the GREATEST concern?

- Most employees use laptops.
- A packet filtering firewall is used.
- The IP address space is smaller than the number of PCs.
- Access to a network port is not restricted.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Unrestricted access to network ports allows anyone to connect to the internal network, posing significant security risks. The other conditions, while concerning, do not present the same level of exposure.

QUESTION 637
An IS auditor is performing a network security review of a telecom company that provides Internet connection services to shopping malls for their wireless customers. The company uses Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned if a hacker:

- Compromises the Wireless Application Protocol (WAP) gateway.
- Installs a sniffing program in front of the server.
- Steals a customer's PDA.
- Listens to the wireless transmission.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
If the WAP gateway is compromised, encrypted messages must be decrypted for transmission, exposing them to potential interception. Other options present risks but do not compromise the security of all messages.

QUESTION 638
Which of the following BEST reduces the ability of one device to capture the packets that are meant for another device?

- Filters
- Switches
- Routers
- Firewalls

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Switches transmit packets specifically to the intended devices, minimizing the risk of interception by other devices on the network.

QUESTION 639
In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

- Diskless workstations

- Data encryption techniques
- Network monitoring devices
- Authentication systems

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Network monitoring devices inspect traffic and can identify client addresses, serving as a detective control for unauthorized access.

QUESTION 640
When reviewing system parameters, an IS auditor's PRIMARY concern should be that:

- They are set to meet security and performance requirements.
- Changes are recorded in an audit trail and periodically reviewed.
- Changes are authorized and supported by appropriate documents.
- Access to parameters in the system is restricted.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The primary concern should be ensuring parameters meet security and performance requirements, as improper settings can negate the effectiveness of other controls.

QUESTION 641
Which of the following is a control over component communication failure/errors?

- Restricting operator access and maintaining audit trails
- Monitoring and reviewing system engineering activity
- Providing network redundancy
- Establishing physical barriers to the data transmitted over the network

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Network redundancy helps prevent communication failures by providing alternative paths for data transmission.

QUESTION 642
An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

- Electromagnetic interference (EMI)
- Cross-talk
- Dispersion
- Attenuation

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Attenuation is the weakening of signals over distance, which can lead to communication problems in a UTP network.

QUESTION 643
Which of the following line media would provide the BEST security for a telecommunication network?

- Broadband network digital transmission
- Baseband network
- Dial-up
- Dedicated lines

Correct Answer: D

Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Dedicated lines are not shared, reducing the risk of interception and ensuring better security.

QUESTION 644
Which of the following types of firewalls would BEST protect a network from an internet attack?

- Screened subnet firewall
- Application filtering gateway
- Packet filtering router
- Circuit-level gateway

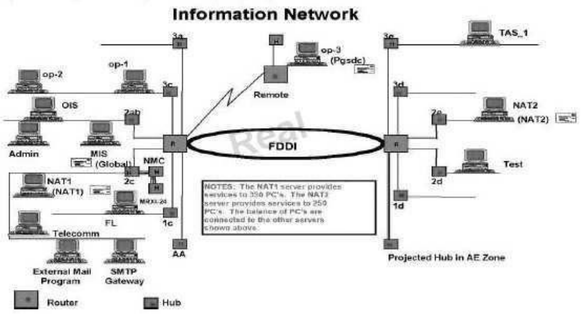
Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
A screened subnet firewall provides comprehensive security by filtering traffic based on multiple criteria.

QUESTION 645
Neural networks are effective in detecting fraud because they can:

- Discover new trends since they are inherently linear.
- Solve problems where large and general sets of training data are not obtainable.
- Attack problems that require consideration of a large number of input variables.
- Make assumptions about the shape of any curve relating variables to the output.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Neural networks excel at processing complex relationships with numerous variables, making them effective for fraud detection.

QUESTION 646



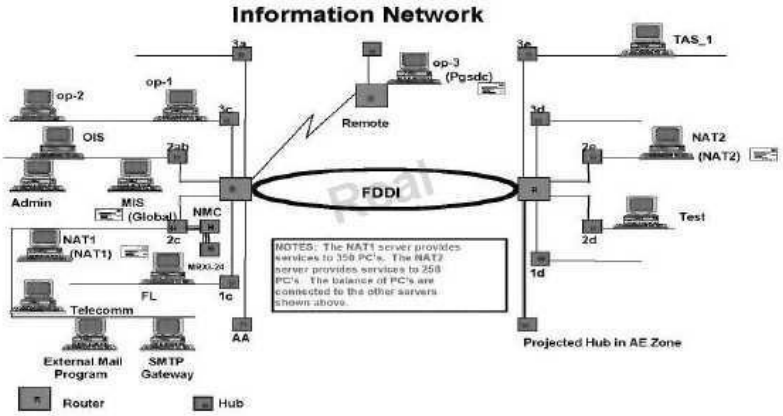
Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?

- No firewalls are needed
- Op-3 location only
- MIS (Global) and NAT2
- SMTP Gateway and op-3

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The objective of a firewall is to protect a trusted network from an untrusted network; therefore, firewalls should

be installed at locations with external connections. All other answers are either incomplete or refer to internal connections.

QUESTION 647

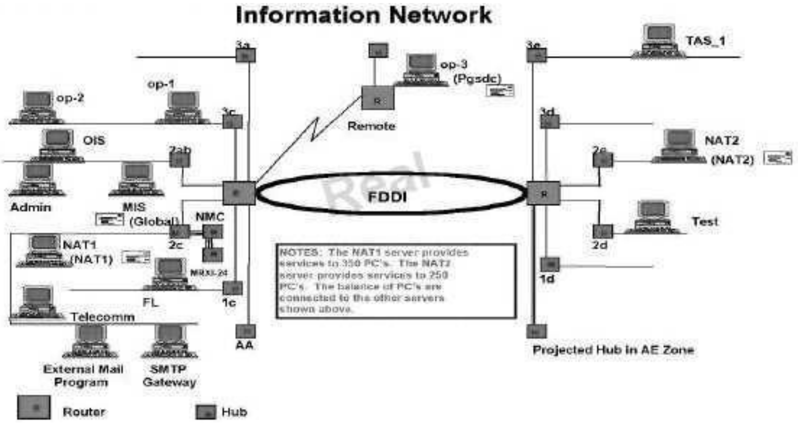


For locations 3a, 1d, and 3d, the diagram indicates hubs with lines that appear to be open and active. Assuming that is true, what control, if any, should be recommended to mitigate this weakness?

- Intelligent hub
- Physical security over the hubs
- Physical security and an intelligent hub
- No controls are necessary since this is not a weakness

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Open hubs represent a significant control weakness because they allow easy access to the network. An intelligent hub would enable the deactivation of individual ports while keeping others active. Additionally, physical security would enhance protection over the active hubs.

QUESTION 648



In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?

- Virus attack
- Performance degradation
- Poor management controls
- Vulnerability to external hackers

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:

Hubs are internal devices typically without direct external connectivity, making them less vulnerable to hackers. While this may indicate poor management controls, the practice of stacking hubs likely leads to performance degradation.

QUESTION 649

An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

- A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
- Firewall policies are updated based on changing requirements.
- Inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
- The firewall is placed on top of the commercial operating system with all installation options.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The greatest concern when implementing firewalls on commercial operating systems is the potential vulnerabilities that could compromise the firewall's security. Many breaches occur due to vulnerabilities in the underlying OS. Other options are essential practices for maintaining firewall security.

QUESTION 650

In a client-server architecture, a domain name service (DNS) is MOST important because it provides the:

- Address of the domain server.
- Resolution service for the name/address.
- IP addresses for the Internet.
- Domain name system.

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
DNS primarily resolves domain names to IP addresses, enabling easier navigation of the Internet. It translates user-friendly names into the numeric IP addresses used for routing traffic.

QUESTION 651

In what way is a common gateway interface (CGI) MOST often used on a web server?

- Consistent way for transferring data to the application program and back to the user
- Computer graphics imaging method for movies and TV
- Graphic user interface for web design
- Interface to access the private gateway domain

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The common gateway interface (CGI) is a standard for passing user requests to application programs and returning data. It facilitates communication between the web server and applications, especially for form submissions.

QUESTION 652

Receiving an EDI transaction and passing it through the communication's interface stage usually requires:

- Translating and unbundling transactions.
- Routing verification procedures.
- Passing data to the appropriate application system.
- Creating a point of receipt audit log.

Correct Answer: B

Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The communication's interface stage necessitates routing verification procedures to ensure EDI transactions are correctly processed. Other options, while important, do not directly pertain to this stage.

QUESTION 653
Which of the following would be considered an essential feature of a network management system?

- A graphical interface to map the network topology
- Capacity to interact with the Internet to solve problems
- Connectivity to a help desk for advice on difficult issues
- An export facility for piping data to spreadsheets

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
A graphical interface for mapping the network topology is essential for effective network management. Other options may be useful but are not fundamental features of a network management system.

QUESTION 654
The most likely error to occur when implementing a firewall is:

- Incorrectly configuring the access lists.
- Compromising the passwords due to social engineering.
- Connecting a modem to the computers in the network.
- Inadequately protecting the network and server from virus attacks.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Errors in configuring access lists present significant challenges during firewall implementation, leading to the highest likelihood of mistakes. Other options do not apply directly to the initial installation phase of a firewall.

QUESTION 655
When reviewing the implementation of a LAN, an IS auditor should FIRST review the:

- Node list.
- Acceptance test report.
- Network diagram.
- User's list.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
To effectively review a LAN implementation, an IS auditor should first examine the network diagram to confirm the system's structure and design, followed by other elements like the node list and acceptance test report.

QUESTION 656
Which of the following would be the MOST secure firewall system?

- Screened-host firewall
- Screened-subnet firewall
- Dual-homed firewall
- Stateful-inspection firewall

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
A screened-subnet firewall, also known as a demilitarized zone (DMZ), utilizes two packet filtering routers and a

bastion host. This setup provides the most secure firewall system by supporting both network- and application-level security while defining a separate DMZ network.

QUESTION 657
Reconfiguring which of the following firewall types will prevent inward downloading of files through the File Transfer Protocol (FTP)?

- Circuit gateway
- Application gateway
- Packet filter
- Screening router

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
An application gateway firewall effectively prevents specific applications, such as FTP, from entering the organization's network. In contrast, a circuit gateway firewall prevents paths or circuits, not specific applications, from entering the network.

QUESTION 658
Which of the following applet intrusion issues poses the GREATEST risk of disruption to an organization?

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

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Applet intrusion that opens connections from the client machine to other machines on the network poses the greatest risk, potentially leading to denial-of-service attacks and significant disruption of business continuity.

QUESTION 659
Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?

- Simple Network Management Protocol
- File Transfer Protocol
- Simple Mail Transfer Protocol
- Telnet

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The Simple Network Management Protocol (SNMP) provides a means to monitor and control network devices, making it essential for managing configurations and performance.

QUESTION 660
Java applets and ActiveX controls are distributed executable programs that execute in the background of a web browser client. This practice is considered reasonable when:

- a firewall exists.
- a secure web connection is used.
- the source of the executable file is certain.
- the host web site is part of the organization.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:

Acceptance of these executable files should be based on established trust. Knowing the source of the executable file allows for reasonable security, as opposed to relying solely on external defenses like firewalls or secure connections.

QUESTION 661
In large corporate networks having supply partners across the globe, network traffic may continue to rise. The infrastructure components in such environments should be scalable. Which of the following firewall architectures limits future scalability?

- Appliances
- Operating system-based
- Host-based
- Demilitarized

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Firewalls built as appliances have their software embedded in chips, making them less scalable since they cannot be moved to higher capacity servers. In contrast, firewalls based on operating systems or host-based solutions can be scaled more easily.

QUESTION 662
Which of the following types of transmission media provide the BEST security against unauthorized access?

- Copper wire
- Twisted pair
- Fiberoptic cables
- Coaxial cables

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Fiberoptic cables are significantly more secure than other transmission media, as they are less susceptible to unauthorized access compared to copper or coaxial cables.

QUESTION 663
Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

- Review the parameter settings.
- Interview the firewall administrator.
- Review the actual procedures.
- Review the device's log file for recent attacks.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Reviewing the parameter settings provides a strong basis for comparing the firewall's actual configuration to the security policy, offering solid audit evidence.

QUESTION 664
To determine how data are accessed across different platforms in a heterogeneous environment, an IS auditor should FIRST review:

- Business software.
- Infrastructure platform tools.
- Application services.
- System development tools.

Correct Answer: C

Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Application services help isolate system developers from the complexities of IT infrastructure, allowing for a clearer understanding of data access across different platforms.

QUESTION 665
During the requirements definition phase for a database application, performance is listed as a top priority. To access the DBMS files, which of the following technologies should be recommended for optimal I/O performance?

- Storage area network (SAN)
- Network Attached Storage (NAS)
- Network file system (NFS v2)
- Common Internet File System (CIFS)

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
A Storage Area Network (SAN) provides optimal performance by allowing direct access to data stored on storage devices, making it similar to direct attached storage.

QUESTION 666
Reverse proxy technology for web servers should be deployed if:

- HTTP servers' addresses must be hidden.
- Accelerated access to all published pages is required.
- Caching is needed for fault tolerance.
- Bandwidth to the user is limited.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Reverse proxies are primarily designed to hide internal structures from outside access, ensuring that server addresses are not disclosed.

QUESTION 667
When auditing a proxy-based firewall, an IS auditor should:

- Verify that the firewall is not dropping any forwarded packets.
- Review Address Resolution Protocol (ARP) tables for appropriate mapping between media access control (MAC) and IP addresses.
- Verify that the filters applied to services such as HTTP are effective.
- Test whether routing information is forwarded by the firewall.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
A proxy-based firewall acts as an intermediary and does not forward packets, so verifying the effectiveness of the applied filters is crucial.

QUESTION 668
An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?

- Simple Object Access Protocol (SOAP)
- Address Resolution Protocol (ARP)
- Routing Information Protocol (RIP)
- Transmission Control Protocol (TCP)

Correct Answer: B

Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The Address Resolution Protocol (ARP) provides dynamic mapping between IP addresses and MAC addresses, making it essential for detecting unauthorized mappings.

QUESTION 669
An IS auditor examining the configuration of an operating system to verify the controls should review the:

- Transaction logs.
- Authorization tables.
- Parameter settings.
- Routing tables.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Parameter settings are crucial for determining how a system runs, and improper implementation can lead to unauthorized access and data corruption.

QUESTION 670
When reviewing an implementation of a VoIP system over a corporate WAN, an IS auditor should expect to find:

- An integrated services digital network (ISDN) data link.
- Traffic engineering.
- Wired equivalent privacy (WEP) encryption of data.
- Analog phone terminals.

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Traffic engineering is necessary to manage network performance and ensure quality of service for VoIP over a WAN, protecting it from packet loss and latency.

QUESTION 671
Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?

- Session keys are dynamic
- Private symmetric keys are used
- Keys are static and shared
- Source addresses are not encrypted or authenticated

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
WPA uses dynamic session keys, achieving stronger encryption than Wired Equivalent Privacy (WEP), which operates with static keys (the same key is used for everyone in the wireless network). All other choices are weaknesses of WEP.

QUESTION 672
During the audit of a database server, which of the following would be considered the GREATEST exposure?

- The password does not expire on the administrator account
- Default global security settings for the database remain unchanged
- Old data have not been purged
- Database activity is not fully logged

Correct Answer: B

Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Default security settings for the database could allow issues like blank user passwords or passwords that were the same as the username. Logging all database activity is not practical. Failure to purge old data may present a performance issue but is not an immediate security concern. Choice A is an exposure but not as serious as B.

QUESTION 673
Which significant risk is introduced by running the file transfer protocol (FTP) service on a server in a demilitarized zone (DMZ)?

- A user from within could send a file to an unauthorized person.
- FTP services could allow a user to download files from unauthorized sources.
- A hacker may be able to use the FTP service to bypass the firewall.
- FTP could significantly reduce the performance of a DMZ server.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Since FTP is considered an insecure protocol, it should not be installed on a server in a DMZ. FTP could allow an unauthorized user to gain access to the network. Sending files to an unauthorized person and the risk of downloading unauthorized files are not as significant as having a firewall breach. The presence of the utility does not reduce the performance of a DMZ server; therefore, performance degradation is not a threat.

QUESTION 674
The MAIN reason for requiring that all computer clocks across an organization be synchronized is to:

- Prevent omission or duplication of transactions.
- Ensure smooth data transition from client machines to servers.
- Ensure that e-mail messages have accurate time stamps.
- Support the incident investigation process.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
During an investigation of incidents, audit logs are used as evidence, and the time stamp information in them is useful. If the clocks are not synchronized, investigations will be more difficult because a timeline of events might not be easily established. Time-stamping a transaction has nothing to do with the update itself. Therefore, the possibility of omission or duplication of transactions does not exist. Data transfer has nothing to do with the timestamp. While the timestamp on an email may not be accurate, this is not a significant issue.

QUESTION 675
When reviewing the configuration of network devices, an IS auditor should FIRST identify:

- The best practices for the type of network devices deployed.
- Whether components of the network are missing.
- The importance of the network device in the topology.
- Whether subcomponents of the network are being used appropriately.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The first step is to understand the importance and role of the network device within the organization's network topology. After understanding the devices in the network, the best practice for using the device should be reviewed to ensure that there are no anomalies within the configuration. Identification of which component or subcomponent is missing or being used inappropriately can only be known upon reviewing and understanding the topology and the best practice for the deployment of the device in the network.

QUESTION 676

Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?

- System analysis
- Authorization of access to data
- Application programming
- Data administration

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The application owner is responsible for authorizing access to data. Application development and programming are functions of the IS department. Similarly, system analysis should be performed by qualified persons in IS who have knowledge of IS and user requirements. Data administration is a specialized function related to database management systems and should be performed by qualified database administrators.

QUESTION 677
Accountability for the maintenance of appropriate security measures over information assets resides with the:

- Security administrator.
- Systems administrator.
- Data and systems owners.
- Systems operations group.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

QUESTION 678
The GREATEST risk when end users have access to a database at its system level, instead of through the application, is that the users can:

- Make unauthorized changes to the database directly, without an audit trail.
- Make use of a system query language (SQL) to access information.
- Remotely access the database.
- Update data without authentication.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Having access to the database could provide access to database utilities, which can update the database without an audit trail and without using the application. Using SQL only provides read access to information; in a networked environment, accessing the database remotely does not make a difference. What is critical is what is possible or completed through this access. To access a database, it is necessary that a user is authenticated using a user ID.

QUESTION 679
To determine who has been given permission to use a particular system resource, an IS auditor should review:

- Activity lists.
- Access control lists.
- Logon ID lists.
- Password lists.

Correct Answer: B

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

QUESTION 680
Which of the following is the MOST effective control when granting temporary access to vendors?

- Vendor access corresponds to the service level agreement (SLA).
- User accounts are created with expiration dates and are based on services provided.
- Administrator access is provided for a limited period.
- User IDs are deleted when the work is completed.

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

QUESTION 681
During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

- An unauthorized user may use the ID to gain access.
- User access management is time-consuming.
- Passwords are easily guessed.
- User accountability may not be established.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The use of a single user ID by more than one individual precludes knowing who, in fact, used that ID to access a system; therefore, it is literally impossible to hold anyone accountable. All user IDs, not just shared IDs, can be used by unauthorized individuals. Access management would not be any different with shared IDs, and shared user IDs do not necessarily have easily guessed passwords.

QUESTION 682
Which of the following satisfies a two-factor user authentication?

- Iris scanning plus fingerprint scanning
- Terminal ID plus global positioning system (GPS)
- A smart card requiring the user's PIN
- User ID along with password

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
A smart card addresses what the user has. This is generally used in conjunction with testing what the user knows, e.g., a keyboard password or personal identification number (PIN). Proving who the user is usually requires a biometrics method, such as fingerprint, iris scan, or voice verification, to prove biology. This is not a two-factor user authentication, because it proves only who the user is. A global positioning system (GPS) receiver reports on where the user is. The use of an ID and password (what the user knows) is a single-factor user authentication.

QUESTION 683

What is the MOST effective method of preventing unauthorized use of data files?

- Automated file entry
- Tape librarian
- Access control software
- Locked library

Correct Answer: C

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Access control software is an active control designed to prevent unauthorized access to data.

QUESTION 684

Which of the following is the PRIMARY safeguard for securing software and data within an information processing facility?

- Security awareness
- Reading the security policy
- Security committee
- Logical access controls

Correct Answer: D

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

To retain a competitive advantage and meet basic business requirements, organizations must ensure that the integrity of the information stored on their computer systems preserves the confidentiality of sensitive data and ensures the continued availability of their information systems. To meet these goals, logical access controls must be in place. Awareness (choice A) itself does not protect against unauthorized access or disclosure of information. Knowledge of an information systems security policy (choice B), which should be known by the organization's employees, would help to protect information, but would not prevent unauthorized access. A security committee (choice C) is key to the protection of information assets, but would address security issues from a broader perspective.

QUESTION 685

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

- Provides an audit trail
- Can be used in a switchboard environment
- Permits unlimited user mobility
- Allows call forwarding

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

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

QUESTION 686

When reviewing an organization's logical access security, which of the following should be of MOST concern to an IS auditor?

- Passwords are not shared.
- Password files are not encrypted.
- Redundant logon IDs are deleted.

- The allocation of logon IDs is controlled.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
When evaluating the technical aspects of logical security, unencrypted files represent the greatest risk. The sharing of passwords, checking for the redundancy of logon IDs, and proper logon ID procedures are essential, but they are less important than ensuring that the password files are encrypted.

QUESTION 687
Passwords should be:

- Assigned by the security administrator for first time logon.
- Changed every 30 days at the discretion of the user.
- Reused often to ensure the user does not forget the password.
- Displayed on the screen so that the user can ensure that it has been entered properly.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Initial password assignment should be done discretely by the security administrator. Passwords should be changed often (e.g., every 30 days); however, changing should not be voluntary, it should be required by the system. Systems should not permit previous passwords to be used again. Old passwords may have been compromised and would thus permit unauthorized access. Passwords should not be displayed in any form.

QUESTION 688
When performing an audit of access rights, an IS auditor should be suspicious of which of the following if allocated to a computer operator?

- Read access to data
- Delete access to transaction data files
- Logged read/execute access to programs
- Update access to job control language/script files

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Deletion of transaction data files should be a function of the application support team, not operations staff. Read access to production data is a normal requirement of a computer operator, as is logged access to programs and access to JCL to control job execution.

QUESTION 689
To prevent unauthorized entry to the data maintained in a dial-up, fast response system, an IS auditor should recommend:

- Online terminals are placed in restricted areas.
- Online terminals are equipped with key locks.
- ID cards are required to gain access to online terminals.
- Online access is terminated after a specified number of unsuccessful attempts.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The most appropriate control to prevent unauthorized entry is to terminate connection after a specified number of attempts. This will deter access through guessing of IDs and passwords. The other choices are physical controls, which are not effective in deterring unauthorized accesses via telephone lines.

QUESTION 690

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

- Exposure is greater since information is available to unauthorized users.
- Operating efficiency is enhanced since anyone can print any report at any time.
- Operating procedures are more effective since information is easily available.
- User friendliness and flexibility is facilitated since there is a smooth flow of information among users.

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

QUESTION 691
Sign-on procedures include the creation of a unique user ID and password. However, an IS auditor discovers that in many cases the username and password are the same. The BEST control to mitigate this risk is to:

- Change the company's security policy.
- Educate users about the risk of weak passwords.
- Build in validations to prevent this during user creation and password change.
- Require a periodic review of matching user ID and passwords for detection and correction.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The compromise of the password is the highest risk. The best control is a preventive control through validation at the time the password is created or changed. Changing the company's security policy and educating users about the risks of weak passwords only provides information to users, but does little to enforce this control. Requiring a periodic review of matching user ID and passwords for detection and ensuring correction is a detective control.

QUESTION 692
The PRIMARY objective of a logical access control review is to:

- Review access controls provided through software.
- Ensure access is granted per the organization's authorities.
- Walk through and assess the access provided in the IT environment.
- Provide assurance that computer hardware is adequately protected against abuse.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The scope of a logical access control review is primarily to determine whether or not access is granted per the organization's authorizations. Choices A and C relate to procedures of a logical access control review, rather than objectives. Choice D is relevant to a physical access control review.

QUESTION 693
Naming conventions for system resources are important for access control because they:

- Ensure that resource names are not ambiguous.
- Reduce the number of rules required to adequately protect resources.
- Ensure that user access to resources is clearly and uniquely identified.
- Ensure that internationally recognized names are used to protect resources.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Naming conventions for system resources are important for the efficient administration of security controls. The

conventions can be structured, so resources beginning with the same high-level qualifier can be governed by one or more generic rules. This reduces the number of rules required to adequately protect resources, which in turn facilitates security administration and maintenance efforts. Reducing the number of rules required to protect resources allows for the grouping of resources and files by application, which makes it easier to provide access. Ensuring that resource names are not ambiguous cannot be achieved through the use of naming conventions. Ensuring the clear and unique identification of user access to resources is handled by access control rules, not naming conventions. Internationally recognized names are not required to control access to resources. Naming conventions tend to be based on how each organization wants to identify its resources.

QUESTION 694

Which of the following exposures could be caused by a line grabbing technique?

- Unauthorized data access
- Excessive CPU cycle usage
- Lockout of terminal polling
- Multiplexor control dysfunction

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Line grabbing will enable eavesdropping, thus allowing unauthorized data access; it will not necessarily cause multiplexor dysfunction, excessive CPU usage, or lockout of terminal polling.

QUESTION 695

Electromagnetic emissions from a terminal represent an exposure because they:

- Affect noise pollution.
- Disrupt processor functions.
- Produce dangerous levels of electric current.
- Can be detected and displayed.

Correct Answer: D

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

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

QUESTION 696

Security administration procedures require read-only access to:

- Access control tables.
- Security log files.
- Logging options.
- User profiles.

Correct Answer: B

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Security administration procedures require read-only access to security log files to ensure that, once generated, the logs are not modified. Logs provide evidence and track suspicious transactions and activities. Security administration procedures require write access to access control tables to manage and update the privileges according to authorized business requirements. Logging options require write access to allow the administrator to update how transactions and user activities are monitored, captured, stored, processed, and reported.

QUESTION 697

With the help of a security officer, granting access to data is the responsibility of:

- Data owners.
- Programmers.

- System analysts.
- Librarians.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Data owners are responsible for the use of data. Written authorization for users to gain access to computerized information should be provided by the data owners. Security administration, with the owners' approval, sets up access rules stipulating which users or groups of users are authorized to access data or files and the level of authorized access (e.g., read or update).

QUESTION 698
The FIRST step in data classification is to:

- Establish ownership.
- Perform a criticality analysis.
- Define access rules.
- Create a data dictionary.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Data classification is necessary to define access rules based on a need-to-do and need-to-know basis. The data owner is responsible for defining the access rules; therefore, establishing ownership is the first step in data classification. The other choices are incorrect. A criticality analysis is required for the protection of data, which takes input from data classification. Access definition is complete after data classification, and input for a data dictionary is prepared from the data classification process.

QUESTION 699
Which of the following provides the framework for designing and developing logical access controls?

- Information systems security policy
- Access control lists
- Password management
- System configuration files

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The information systems security policy developed and approved by an organization's top management is the basis upon which logical access control is designed and developed. Access control lists, password management, and systems configuration files are tools for implementing the access controls.

QUESTION 700
A hacker could obtain passwords without the use of computer tools or programs through the technique of:

- Social engineering.
- Sniffers.
- Back doors.
- Trojan horses.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Social engineering is based on the divulgence of private information through dialogues and interviews.

QUESTION 701
The reliability of an application system's audit trail may be questionable if:

- user IDs are recorded in the audit trail.
- the security administrator has read-only rights to the audit file.
- date and time stamps are recorded when an action occurs.
- users can amend audit trail records when correcting system errors.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
An audit trail is not effective if the details in it can be amended.

QUESTION 702
Which of the following user profiles should be of MOST concern to an IS auditor when performing an audit of an EFT system?

- Three users with the ability to capture and verify their own messages
- Five users with the ability to capture and send their own messages
- Five users with the ability to verify other users and to send their own messages
- Three users with the ability to capture and verify the messages of other users and to send their own messages

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The ability of one individual to capture and verify messages represents inadequate segregation since messages can be taken as correct and as if they had already been verified.

QUESTION 703
An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as:

- critical.
- vital.
- sensitive.
- noncritical.

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

QUESTION 704
The implementation of access controls FIRST requires:

- a classification of IS resources.
- the labeling of IS resources.
- the creation of an access control list.
- an inventory of IS resources.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The implementation of access controls begins with an inventory of IS resources to understand what needs to be protected.

QUESTION 705

Which of the following is an example of the defense-in-depth security principle?

- Using two firewalls of different vendors to consecutively check the incoming network traffic
- Using a firewall as well as logical access controls on the hosts to control incoming network traffic
- Having no physical signs on the outside of a computer center building
- Using two firewalls in parallel to check different types of incoming traffic

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:

Defense in depth means using different security mechanisms that back each other up. When network traffic passes the firewall unintentionally, the logical access controls form a second line of defense. Using two firewalls of different vendors to consecutively check the incoming network traffic is an example of diversity in defense. The firewalls are the same security mechanisms. By using two different products, the probability of both products having the same vulnerabilities is diminished. Having no physical signs on the outside of a computer center building is a single security measure. Using two firewalls in parallel to check different types of incoming traffic is a single security mechanism and therefore no different than having a single firewall checking all traffic.

QUESTION 706

Which of the following would be the BEST access control procedure?

- The data owner formally authorizes access, and an administrator implements the user authorization tables.
- Authorized staff implements the user authorization tables and the data owner sanctions them.
- The data owner and an IS manager jointly create and update the user authorization tables.
- The data owner creates and updates the user authorization tables.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:

The data owner holds the privilege and responsibility for formally establishing the access rights. An IS administrator should then implement or update user authorization tables. Choice B alters the desirable order. Choice C is not a formal procedure for authorizing access.

QUESTION 707

Which of the following would MOST effectively reduce social engineering incidents?

- Security awareness training
- Increased physical security measures
- E-mail monitoring policy
- Intrusion detection systems

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:

Social engineering exploits human nature and weaknesses to obtain information and access privileges. By increasing employee awareness of security issues, it is possible to reduce the number of successful social engineering incidents. In most cases, social engineering incidents do not require the physical presence of the intruder. Therefore, increased physical security measures would not prevent the intrusion. An e-mail monitoring policy informs users that all e-mail in the organization is subject to monitoring; it does not protect the users from potential security incidents and intruders. Intrusion detection systems are used to detect irregular or abnormal traffic patterns.

QUESTION 708

An information security policy stating that "the display of passwords must be masked or suppressed" addresses which of the following attack methods?

- Piggybacking

- Dumpster diving
- Shoulder surfing
- Impersonation

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

QUESTION 709
To ensure compliance with a security policy requiring that passwords be a combination of letters and numbers, an IS auditor should recommend that:

- the company policy be changed.
- passwords are periodically changed.
- an automated password management tool be used.
- security awareness training is delivered.

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

QUESTION 710
An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:

- more than one individual can claim to be a specific user.
- there is no way to limit the functions assigned to users.
- user accounts can be shared.
- users have a need-to-know privilege.

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

QUESTION 711
An IS auditor reviewing digital rights management (DRM) applications should expect to find an extensive use for which of the following technologies?

- Digitalized signatures
- Hashing
- Parsing
- Steganography

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Steganography is a technique for concealing the existence of messages or information. An increasingly important steganographical technique is digital watermarking, which hides data within data, e.g., by encoding rights information in a picture or music file without altering the picture or music's perceivable aesthetic qualities. Digitalized signatures are not related to digital rights management. Hashing creates a message hash or digest, which is used to ensure the integrity of the message; it is usually considered a part of cryptography. Parsing is the process of splitting up a continuous stream of characters for analytical purposes and is widely applied in the design of programming languages or in data entry editing.

QUESTION 712
The information security policy that states "each individual must have their badge read at every controlled door" addresses which of the following attack methods?

- Piggybacking
- Shoulder surfing
- Dumpster diving
- Impersonation

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger; if every employee must have their badge read at every controlled door, no unauthorized person could enter the sensitive area. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas using piggybacking, but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee trying to retrieve the desired information. Some forms of social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

QUESTION 713
Which of the following presents an inherent risk with no distinct identifiable preventive controls?

- Piggybacking
- Viruses
- Data diddling
- Unauthorized application shutdown

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Data diddling involves changing data before they are entered into the computer. It is one of the most common abuses because it requires limited technical knowledge and occurs before computer security can protect the data. There are only compensating controls for data diddling. Piggybacking is the act of following an authorized person through a secured door and can be prevented by the use of deadman doors. Logical piggybacking is an attempt to gain access through someone who has the rights, e.g., electronically attaching to an authorized telecommunication link to possibly intercept transmissions. This could be prevented by encrypting the message. Viruses are malicious program code inserted into another executable code that can self-replicate and spread from computer to computer via sharing of computer diskettes, transfer of logic over telecommunication lines, or direct contact with an infected machine. Antiviral software can be used to protect the computer against viruses. The shutdown of an application can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up

line) to the computer. Only individuals knowing the high-level logon ID and password can initiate the shutdown process, which is effective if there are proper access controls.

QUESTION 714

Which of the following is a general operating system access control function?

- Creating database profiles
- Verifying user authorization at a field level
- Creating individual accountability
- Logging database access activities for monitoring access violations

Correct Answer: C

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Creating individual accountability is the function of the general operating system. Creating database profiles, verifying user authorization at a field level, and logging database access activities for monitoring access violations are all database-level access control functions.

QUESTION 715

Which of the following BEST restricts users to those functions needed to perform their duties?

- Application level access control
- Data encryption
- Disabling floppy disk drives
- Network monitoring device

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

The use of application-level access control programs is a management control that restricts access by limiting users to only those functions needed to perform their duties. Data encryption and disabling floppy disk drives can restrict users to specific functions, but are not the best choices. A network monitoring device is a detective control, not a preventive control.

QUESTION 716

For a discretionary access control to be effective, it must:

- operate within the context of mandatory access controls.
- operate independently of mandatory access controls.
- enable users to override mandatory access controls when necessary.
- be specifically permitted by the security policy.

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Discretionary access control (DAC) operates within the framework established by mandatory access controls (MAC). While DAC allows users some flexibility in controlling access, it still functions under the prohibition principle of MAC, where anything not expressly permitted is forbidden.

QUESTION 717

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

- Kerberos
- Vitality detection
- Multimodal biometrics
- Before-image/after-image logging

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Kerberos is a network authentication protocol that provides secure authentication, thereby preventing unauthorized access to the database. Vitality detection and multimodal biometrics primarily defend against spoofing, while before-image/after-image logging is a detective control, not preventative.

QUESTION 718
From a control perspective, the PRIMARY objective of classifying information assets is to:

- establish guidelines for the level of access controls that should be assigned.
- ensure access controls are assigned to all information assets.
- assist management and auditors in risk assessment.
- identify which assets need to be insured against losses.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Classifying information assets helps establish guidelines for access controls based on sensitivity and criticality. While it assists in risk assessment, the primary objective is to provide a framework for access control.

QUESTION 719
An organization has been recently downsized. In light of this, an IS auditor decides to test logical access controls. The IS auditor's PRIMARY concern should be that:

- all system access is authorized and appropriate for an individual's role and responsibilities.
- management has authorized appropriate access for all newly-hired individuals.
- only the system administrator has authority to grant or modify access to individuals.
- access authorization forms are used to grant or modify access to individuals.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Given the rapid personnel changes during downsizing, the auditor must ensure that access rights are still appropriate for each individual's new role and responsibilities and that access is revoked for those no longer with the organization.

QUESTION 720
The logical exposure associated with the use of a checkpoint restart procedure is:

- denial of service.
- an asynchronous attack.
- wire tapping.
- computer shutdown.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Checkpoint restart procedures can be susceptible to asynchronous attacks, where an attacker may manipulate parameters saved at checkpoints, potentially gaining higher access levels upon restart.

QUESTION 721
Inadequate programming and coding practices introduce the risk of:

- phishing.
- buffer overflow exploitation.
- SYN flood.
- brute force attacks.

Correct Answer: B

Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Buffer overflow vulnerabilities arise from poor coding practices, allowing attackers to exploit these weaknesses. Phishing, SYN floods, and brute force attacks are not directly related to programming practices.

QUESTION 722
Which of the following would prevent unauthorized changes to information stored in a server's log?

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

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Using write-once media ensures the log cannot be altered once written. Write protection can be bypassed by privileged users, and duplicate logs or printed logs do not prevent modifications to the original.

QUESTION 723
After reviewing its business processes, a large organization is deploying a new web application based on VoIP technology. Which of the following is the MOST appropriate approach for implementing access control that will facilitate security management of the VoIP web application?

- Fine-grained access control
- Role-based access control (RBAC)
- Access control lists
- Network/service access control

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
RBAC is suitable for large systems, enabling effective management of user access based on roles. Fine-grained access and access control lists may not scale efficiently for enterprise-wide systems.

QUESTION 724
In an online banking application, which of the following would BEST protect against identity theft?

- Encryption of personal password
- Restricting the user to a specific terminal
- Two-factor authentication
- Periodic review of access logs

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Two-factor authentication enhances security by requiring two forms of identification, making it significantly harder for unauthorized individuals to impersonate legitimate users.

QUESTION 725
Which of the following is the BEST method for preventing the leakage of confidential information in a laptop computer?

- Encrypt the hard disk with the owner's public key.
- Enable the boot password (hardware-based password).
- Use a biometric authentication device.
- Use two-factor authentication to log on to the notebook.

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Encrypting the hard disk with a strong key ensures that confidential information remains secure, even if the device is lost. Authentication methods do not prevent data leakage if the device is physically compromised.

QUESTION 726

The responsibility for authorizing access to application data should be with the:

- data custodian.
- database administrator (DBA).
- data owner.
- security administrator.

Correct Answer: C

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Data owners are responsible for granting access to their data. DBAs manage databases, and security administrators implement security policies, but data ownership confers the authority for access.

QUESTION 727

During an audit of the logical access control of an ERP financial system, an IS auditor found some user accounts shared by multiple individuals. The user IDs were based on roles rather than individual identities. What should the IS auditor do next?

- Look for compensating controls.
- Review financial transactions logs.
- Review the scope of the audit.
- Ask the administrator to disable these accounts.

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

The auditor should evaluate the effectiveness of compensating controls since the best practice is to have unique user IDs for accountability. Other actions might disrupt necessary access without understanding the context.

QUESTION 728

Minimum password length and password complexity verification are examples of:

- detection controls.
- control objectives.
- audit objectives.
- control procedures.

Correct Answer: D

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

These are control procedures established to ensure users create strong passwords, thus serving as preventive measures against unauthorized access.

QUESTION 729

An IS auditor finds that a DBA has read and write access to production data. The IS auditor should:

- accept the DBA access as a common practice.
- assess the controls relevant to the DBA function.
- recommend the immediate revocation of the DBA access to production data.
- review user access authorizations approved by the DBA.

Correct Answer: B

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Evaluating the controls surrounding DBA access is crucial, as such access can be necessary for legitimate tasks. Revocation should not be immediate without understanding the access's context.

QUESTION 730

When using a universal storage bus (USB) flash drive to transport confidential corporate data to an offsite location, an effective control would be to:

- carry the flash drive in a portable safe.
- assure management that you will not lose the flash drive.
- request that management deliver the flash drive by courier.
- encrypt the folder containing the data with a strong key.

Correct Answer: D

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Encrypting the data on the flash drive ensures its security, regardless of physical loss. Other methods do not adequately protect against data breaches if the device is lost or stolen.

QUESTION 731

A business application system accesses a corporate database using a single ID and password embedded in a program. Which would provide efficient access control?

- Apply role-based permissions within the application system.
- Introduce a secondary authentication method such as card swipe.
- Have users input the ID and password for each database transaction.
- Set an expiration period for the database password embedded in the program.

Correct Answer: Apply role-based permissions within the application system.

Section: PROTECTION OF INFORMATION ASSETS

Explanation: Role-based access control effectively manages permissions by assigning roles to users, addressing the main issue of user permissions.

QUESTION 732

Which is the BEST practice to ensure that access authorizations are still valid?

- Information owner provides authorization for users to gain access.
- Identity management is integrated with human resource processes.
- Information owners periodically review the access controls.
- An authorization matrix is used to establish validity of access.

Correct Answer: Identity management is integrated with human resource processes.

Section: PROTECTION OF INFORMATION ASSETS

Explanation: This integration ensures timely adjustments to access rights when personnel changes occur, reducing risks from authorization creep.

QUESTION 733

What would be of GREATEST concern during a forensic investigation after a technical lead leaves the organization?

- Audit logs are not enabled for the system.
- A logon ID for the technical lead still exists.
- Spyware is installed on the system.
- A Trojan is installed on the system.

Correct Answer: Audit logs are not enabled for the system.

Section: PROTECTION OF INFORMATION ASSETS

Explanation: Without audit logs, misuse of the logon ID is difficult to prove, hindering investigation efforts.

QUESTION 734

What would be an effective access control for an ERP application?

- User-level permissions.
- Role-based.
- Fine-grained.
- Discretionary.

Correct Answer: Role-based.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Role-based access control simplifies management by grouping users, while user-level permissions create overhead.

QUESTION 735
What should be the GREATEST concern regarding portable media used by employees?

- The copying of sensitive data on them.
- The copying of songs and videos on them.
- The cost of these devices multiplied by all the employees could be high.
- They facilitate the spread of malicious code through the corporate network.

Correct Answer: The copying of sensitive data on them.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Data leakage is a significant risk, especially sensitive information, if devices are lost or stolen.

QUESTION 736
Who should authorize access rights to production data and systems?

- Process owners.
- System administrators.
- Security administrator.
- Data owners.

Correct Answer: Data owners.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Data owners are responsible for safeguarding and granting access to production data on a need-to-know basis.

QUESTION 737
An IS auditor has completed a network audit. Which of the following is the MOST significant logical security finding?

- Network workstations are not disabled automatically after a period of inactivity.
- Wiring closets are left unlocked.
- Network operating manuals and documentation are not properly secured.
- Network components are not equipped with an uninterruptible power supply.

Correct Answer: Network workstations are not disabled automatically after a period of inactivity.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Disabling inactive workstations restricts unauthorized access, making it a critical finding in logical security.

QUESTION 738
Which of the following would MOST effectively enhance the security of a challenge-response-based authentication system?

- Selecting a more robust algorithm to generate challenge strings.
- Implementing measures to prevent session hijacking attacks.
- Increasing the frequency of associated password changes.
- Increasing the length of authentication strings.

Correct Answer: Implementing measures to prevent session hijacking attacks.

Section: PROTECTION OF INFORMATION ASSETS
Explanation: Addressing the risk of session hijacking is critical for the effectiveness of challenge-response authentication.

QUESTION 739
Which of the following should an IS auditor recommend for the protection of specific sensitive information stored in the data warehouse?

- Implement column- and row-level permissions.
- Enhance user authentication via strong passwords.
- Organize the data warehouse into subject matter-specific databases.
- Log user access to the data warehouse.

Correct Answer: Implement column- and row-level permissions.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Column- and row-level security can prevent unauthorized access to sensitive data, providing a fine-grained security model.

QUESTION 740
The responsibility for authorizing access to a business application system belongs to the:

- Data owner.
- Security administrator.
- IT security manager.
- Requestor's immediate supervisor.

Correct Answer: Data owner.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Data owners are responsible for authorizing access to applications and backend databases.

QUESTION 741
An organization has created a policy that defines the types of websites that users are forbidden to access. What is the MOST effective technology to enforce this policy?

- Stateful inspection firewall.
- Web content filter.
- Web cache server.
- Proxy server.

Correct Answer: Web content filter.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: A web content filter can accept or deny web communications based on configured rules, effectively enforcing access policies.

QUESTION 742
What would be the MOST effective control for enforcing accountability among database users accessing sensitive information?

- Implement a log management process.
- Implement a two-factor authentication.
- Use table views to access sensitive data.
- Separate database and application servers.

Correct Answer: Implement a log management process.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: A log management process creates and stores logs with pertinent information, enforcing accountability by tracking user actions.

QUESTION 743

Which of the following intrusion detection systems (IDSs) monitors the general patterns of activity and traffic on a network and creates a database?

- Signature-based.
- Neural networks-based.
- Statistical-based.
- Host-based.

Correct Answer: Neural networks-based.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Neural networks-based IDSs monitor general patterns of activity, similar to statistical models but with self-learning capabilities.

QUESTION 744
The MOST important difference between hashing and encryption is that hashing:

- Is irreversible.
- Output is the same length as the original message.
- Is concerned with integrity and security.
- Is the same at the sending and receiving end.

Correct Answer: Is irreversible.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Hashing creates a one-way output that cannot be reversed, unlike encryption, which is reversible.

QUESTION 745
Which of the following cryptography options would increase overhead/cost?

- The encryption is symmetric rather than asymmetric.
- A long asymmetric encryption key is used.
- The hash is encrypted rather than the message.
- A secret key is used.

Correct Answer: A long asymmetric encryption key is used.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Longer asymmetric encryption keys require significantly more processing time, increasing overhead.

QUESTION 746
The MOST important success factor in planning a penetration test is:

- The documentation of the planned testing procedure.
- Scheduling and deciding on the timed length of the test.
- The involvement of the management of the client organization.
- The qualifications and experience of staff involved in the test.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation: The most important part of planning any penetration test is the involvement of the management of the client organization. Penetration testing without management approval could reasonably be considered espionage and is illegal in many jurisdictions.

QUESTION 747
Which of the following virus prevention techniques can be implemented through hardware?

- Remote booting
- Heuristic scanners
- Behavior blockers
- Immunizers

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Remote booting (e.g., diskless workstations) is a method of preventing viruses and can be implemented through hardware. Behavior blockers are detection-based rather than prevention-based, and choices B and D are not hardware-based.

QUESTION 748
Which of the following append themselves to files as a protection against viruses?

- Behavior blockers
- Cyclical redundancy checkers (CRCs)
- Immunizers
- Active monitors

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Immunizers defend against viruses by appending sections of themselves to files. They continuously check the file for changes and report changes as possible viral behavior.

QUESTION 749
Which of the following acts as a decoy to detect active internet attacks?

- Honeypots
- Firewalls
- Trapdoors
- Traffic analysis

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Honeypots are computer systems set up to attract and trap individuals attempting to penetrate systems. They help gather data on attack methods to improve future security measures.

QUESTION 750
A certificate authority (CA) can delegate the processes of:

- Revocation and suspension of a subscriber's certificate.
- Generation and distribution of the CA public key.
- Establishing a link between the requesting entity and its public key.
- Issuing and distributing subscriber certificates.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Establishing a link between the requesting entity and its public key is typically a function of a registration authority, which can be delegated by the CA. Other functions, like revocation and key management, are handled directly by the CA.

QUESTION 751
Which of the following results in a denial-of-service attack?

- Brute force attack
- Ping of death
- Leapfrog attack
- Negative acknowledgement (NAK) attack

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation: A Ping of Death attack sends a packet larger than 65 KB without a fragmentation flag, causing a denial of service. Brute force, leapfrog, and NAK attacks have different purposes.

QUESTION 752

Which of the following is the GREATEST advantage of elliptic curve encryption over RSA encryption?

- Computation speed
- Ability to support digital signatures
- Simpler key distribution
- Greater strength for a given key length

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation: The main advantage of elliptic curve encryption over RSA is its faster computation speed, while providing the same level of security with shorter key lengths.

QUESTION 753
Which of the following would be the BEST overall control for an Internet business looking for confidentiality, reliability, and integrity of data?

- Secure Sockets Layer (SSL)
- Intrusion detection system (IDS)
- Public key infrastructure (PKI)
- Virtual private network (VPN)

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation: PKI is the best overall solution for ensuring confidentiality, reliability, and integrity, as it supports encryption, digital signatures, and non-repudiation.

QUESTION 754
To ensure message integrity, confidentiality, and non-repudiation between two parties, the MOST effective method would be to create a message digest by applying a cryptographic hashing algorithm against:

- The entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key, and enciphering the key by using the receiver's public key.
- Any part of the message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key, and enciphering the key using the receiver's public key.
- The entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key, and enciphering both the encrypted message and digest using the receiver's public key.
- The entire message, enciphering the message digest using the sender's private key and enciphering the message using the receiver's public key.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation: This method ensures message integrity by applying a cryptographic hashing algorithm to the entire message and confidentiality through symmetric key encryption, with the symmetric key being encrypted by the receiver’s public key.

QUESTION 755
Which of the following antivirus software implementation strategies would be the MOST effective in an interconnected corporate network?

- Server antivirus software
- Virus walls
- Workstation antivirus software
- Virus signature updating

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Virus walls, integrated with firewalls, detect and remove viruses before they enter the network, providing effective early-stage protection.

QUESTION 756

Which of the following would be of MOST concern to an IS auditor reviewing a virtual private network (VPN) implementation? Computers on the network that are located:

- On the enterprise's internal network.
- At the backup site.
- In employees' homes.
- At the enterprise's remote offices.

Correct Answer: C

Section: PROTECTION OF INFORMATION ASSETS

Explanation: Home computers pose the greatest risk, as they are typically subject to less stringent security policies than corporate-managed systems, increasing the likelihood of introducing vulnerabilities to the VPN.

QUESTION 757

The PRIMARY reason for using digital signatures is to ensure data:

- Confidentiality.
- Integrity.
- Availability.
- Timeliness.

Correct Answer: B

Section: PROTECTION OF INFORMATION ASSETS

Explanation: Digital signatures provide data integrity by ensuring that a document has not been altered after it was signed.

QUESTION 758

Which of the following is an example of a passive attack initiated through the Internet?

- Traffic analysis
- Masquerading
- Denial of service
- E-mail spoofing

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS

Explanation: Passive attacks include activities like traffic analysis and eavesdropping, where the attacker monitors communication without altering it.

QUESTION 759

Transmitting redundant information with each character or frame to facilitate detection and correction of errors is called:

- Feedback error control.
- Block sum check.
- Forward error control.
- Cyclic redundancy check.

Correct Answer: C

Section: PROTECTION OF INFORMATION ASSETS

Explanation: Forward error control transmits extra information with each frame, allowing the receiver to detect and correct errors, making it an efficient method of error control.

QUESTION 760

The security level of a private key system depends on the number of:

- Encryption key bits.
- Messages sent.
- Keys.
- Channels used.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation: The security level of a private key system is directly related to the number of encryption key bits used. The more bits in the key, the harder it is to break the encryption.

QUESTION 761
During what process should router access control lists be reviewed?

- **Environmental review**
- **Network security review**
- **Business continuity review**
- **Data integrity review**

Correct Answer: B
Explanation: Router access control lists should be reviewed during **network security reviews**. This process includes reviewing various network controls such as router access control lists, port scanning, and connections to both internal and external systems. Environmental, business continuity, and data integrity reviews typically do not involve checking router access control lists.

QUESTION 762
Which of the following components is responsible for the collection of data in an intrusion detection system (IDS)?

- **Analyzer**
- **Administration console**
- **User interface**
- **Sensor**

Correct Answer: D
Explanation: In an IDS, **sensors** are responsible for collecting data. **Analyzers** process the collected data to detect possible intrusions. The **administration console** and **user interface** are for managing and interacting with the system but are not directly involved in data collection.

QUESTION 763
Which of the following concerns associated with the World Wide Web would be addressed by a firewall?

- **Unauthorized access from outside the organization**
- **Unauthorized access from within the organization**
- **A delay in Internet connectivity**
- **A delay in downloading using File Transfer Protocol (FTP)**

Correct Answer: A
Explanation: Firewalls are designed to prevent unauthorized access from outside an organization. They act as barriers, blocking unapproved inbound traffic from the internet. They are not intended to address internal access issues or performance-related problems like delays in connectivity or FTP downloads.

QUESTION 764
A digital signature contains a message digest to:

- **Show if the message has been altered after transmission.**
- **Define the encryption algorithm.**
- **Confirm the identity of the originator.**
- **Enable message transmission in a digital format.**

Correct Answer: A
Explanation: The **message digest** included in a digital signature helps ensure data integrity by verifying if the message has been altered. The digest does not define the encryption algorithm or confirm the sender’s identity but ensures that the content remains unchanged during transmission.

QUESTION 765
Which of the following manages the digital certificate life cycle to ensure adequate security and controls exist in digital signature applications related to e-commerce?

- **Registration authority**
- **Certificate authority (CA)**
- **Certification relocation list**
- **Certification practice statement**

Correct Answer: B
Explanation: A **Certificate Authority (CA)** is responsible for managing the lifecycle of digital certificates, including issuance, renewal, and revocation. It also maintains certificate directories and manages the Certificate Revocation List (CRL). A **registration authority** handles administrative tasks like certificate requests but does not manage the certificate lifecycle.

QUESTION 766
A TCP/IP-based environment is exposed to the Internet. Which of the following BEST ensures that complete encryption and authentication protocols exist for protecting information while transmitted?

- **Work is completed in tunnel mode with IP security using the nested services of authentication header (AH) and encapsulating security payload (ESP).**
- **A digital signature with RSA has been implemented.**
- **Digital certificates with RSA are being used.**
- **Work is being completed in TCP services.**

Correct Answer: A
Explanation: Using **tunnel mode with IP security (IPSec)** and employing the **Authentication Header (AH)** and **Encapsulating Security Payload (ESP)** services provides complete encryption and authentication for protecting information. The other options provide either authentication or encryption but not both.

QUESTION 767
Digital signatures require the:

- **Signer to have a public key and the receiver to have a private key.**
- **Signer to have a private key and the receiver to have a public key.**
- **Signer and receiver to have a public key.**
- **Signer and receiver to have a private key.**

Correct Answer: B
Explanation: In digital signature cryptography, the **signer uses a private key** to create the signature, and the **receiver uses the signer's public key** to verify the signature. This ensures that only the signer could have created the signature, and the recipient can confirm its authenticity.

QUESTION 768
The feature of a digital signature that ensures the sender cannot later deny generating and sending the message is called:

- **Data integrity.**
- **Authentication.**
- **Non-repudiation.**
- **Replay protection.**

Correct Answer: C
Explanation: Non-repudiation ensures that the sender cannot deny having generated and sent the message. It confirms the sender's identity and prevents them from claiming otherwise, which is a key feature of digital signatures.

QUESTION 769
An IS auditor doing penetration testing during an audit of internet connections would:

- **Evaluate configurations.**

- **Examine security settings.**
- **Ensure virus-scanning software is in use.**
- **Use tools and techniques available to a hacker.**

Correct Answer: D

Explanation: Penetration testing involves simulating hacker-like attacks on a system using the same tools and techniques a hacker might use. The other options are activities of an IS auditor but are not specific to penetration testing.

QUESTION 770

Which of the following should concern an IS auditor when reviewing security in a client-server environment?

- **Protecting data using an encryption technique**
- **Preventing unauthorized access using a diskless workstation**
- **The ability of users to access and modify the database directly**
- **Disabling floppy drives on the users' machines**

Correct Answer: C

Explanation: An IS auditor should be most concerned about users directly accessing and modifying a database because this could lead to data integrity issues. Other concerns, such as encryption and preventing copying, are secondary to this fundamental security concern.

QUESTION 771

Which of the following is a technique that could be used to capture network user passwords?

- **Encryption**
- **Sniffing**
- **Spoofing**
- **Data destruction**

Correct Answer: B

Explanation: Sniffing is a technique used to capture data packets traversing a network, which can include sensitive information like passwords. **Encryption** prevents unauthorized access to data, **spoofing** involves impersonating another entity, and **data destruction** involves deleting information.

QUESTION 772

Which of the following controls would BEST detect intrusion?

- **User IDs and user privileges are granted through authorized procedures.**
- **Automatic logoff is used when a workstation is inactive for a particular period of time.**
- **Automatic logoff of the system occurs after a specified number of unsuccessful attempts.**
- **Unsuccessful logon attempts are monitored by the security administrator.**

Correct Answer: D

Explanation: Monitoring **unsuccessful logon attempts** helps detect potential intrusions by tracking repeated failed attempts to access a system. The other options are preventative or reactive controls, but do not directly detect intrusion.

QUESTION 773

Which of the following is a feature of an intrusion detection system (IDS)?

- **Gathering evidence on attack attempts**
- **Identifying weaknesses in the policy definition**
- **Blocking access to particular sites on the Internet**
- **Preventing certain users from accessing specific servers**

Correct Answer: A

Explanation: An **IDS** gathers evidence on attack attempts or penetration efforts to identify possible intrusions. **Blocking access** and **preventing user access** are typically functions of a firewall, not an IDS.

QUESTION 774

An IS auditor performing a telecommunication access control review should be concerned PRIMARILY with the:

- **Maintenance of access logs of usage of various system resources.**
- **Authorization and authentication of the user prior to granting access to system resources.**
- **Adequate protection of stored data on servers by encryption or other means.**
- **Accountability system and the ability to identify any terminal accessing system resources.**

Correct Answer: B

Explanation: The primary concern in a **telecommunication access control review** is ensuring **authorization and authentication** are in place before granting access. This is a critical preventive control. Other choices are important but secondary concerns in this context.

QUESTION 775

Which of the following is the MOST effective type of antivirus software?

- **Scanners**
- **Active monitors**
- **Integrity checkers**
- **Vaccines**

Correct Answer: C

Explanation: Integrity checkers are highly effective as they verify the integrity of files by comparing them against a known baseline (often using a CRC or hash function). They can detect changes indicative of virus infections. **Scanners** and **vaccines** require regular updates to remain effective, while **active monitors** can sometimes cause false positives.

QUESTION 776

When using public key encryption to secure data being transmitted across a network:

- **Both the key used to encrypt and decrypt the data are public.**
- **The key used to encrypt is private, but the key used to decrypt the data is public.**
- **The key used to encrypt is public, but the key used to decrypt the data is private.**
- **Both the key used to encrypt and decrypt the data are private.**

Correct Answer: C

Explanation: In **public key encryption** (asymmetric encryption), the **public key** is used to encrypt the data, and the corresponding **private key** is used to decrypt it.

QUESTION 777

The technique used to ensure security in virtual private networks (VPNs) is:

- **Encapsulation**
- **Wrapping**
- **Transform**
- **Encryption**

Correct Answer: A

Explanation: Encapsulation, also known as **tunneling**, is a technique used in VPNs to securely transport data over networks by encapsulating it in another protocol. **Encryption** also plays a role, but encapsulation is the key technique in VPN security.

QUESTION 778

During an audit of a telecommunications system, an IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST effective control for reducing this exposure is:

- **Encryption**
- **Callback modems**
- **Message authentication**
- **Dedicated leased lines**

Correct Answer: A

Explanation: Encryption is the most effective method to protect data in transit from being intercepted. **Callback modems** and **leased lines** offer some security but do not protect the data itself from being intercepted.

QUESTION 779

An internet-based attack using password sniffing can:

- **Enable one party to act as if they are another party.**
- **Cause modification to the contents of certain transactions.**
- **Be used to gain access to systems containing proprietary information.**
- **Result in major problems with billing systems and transaction processing agreements.**

Correct Answer: C

Explanation: Password sniffing allows attackers to gain access to systems containing sensitive information, such as proprietary data. The other options describe different types of attacks, such as **spoofing** and **data modification**.

QUESTION 780

Which of the following controls would be the MOST comprehensive in a remote access network with multiple and diverse subsystems?

- **Proxy server**
- **Firewall installation**
- **Network administrator**
- **Password implementation and administration**

Correct Answer: D

Explanation: Password implementation and administration is the most comprehensive control for a remote access network, as it ensures that only authorized users can access various subsystems. **Firewalls** and **proxy servers** are essential but are more specific controls.

QUESTION 781

An IS auditor notes that an organization's development team has too much access to the production environment. The PRIMARY concern is that this could:

- A. cause unintentional changes to the production environment.
- B. lead to unauthorized changes to business data.
- C. result in segregation of duties (SoD) conflicts.
- D. affect the quality assurance (QA) process.

Correct Answer: C

Explanation: The primary concern when a development team has too much access to the production environment is a segregation of duties (SoD) conflict. Developers with production access could make changes without appropriate approval or testing, leading to unauthorized changes or potentially harmful modifications in a live environment. While the other issues (like unintentional changes, changes to business data, and QA process impacts) are valid concerns, SoD conflicts are the most critical because they compromise internal controls designed to prevent fraud or errors.

QUESTION 782

When planning an audit of a network setup, an IS auditor should give highest priority to obtaining which of the following network documentation?

- A) **Wiring and schematic diagram**
- B) Users' lists and responsibilities
- C) Application lists and their details
- D) Backup and recovery procedures

Correct Answer: A

Explanation: The wiring and schematic diagram of the network is essential for carrying out a network audit. Without it, an audit may not be feasible. While the other documents are important, they are not as critical as understanding the physical and logical network layout.

QUESTION 783

Which of the following encrypt/decrypt steps provides the GREATEST assurance of achieving confidentiality, message integrity, and nonrepudiation by either sender or recipient?

- A) The recipient uses their private key to decrypt the secret key.
- B) The encrypted prehash code and the message are encrypted using a secret key.
- C) The encrypted prehash code is derived mathematically from the message to be sent.
- D) **The recipient uses the sender's public key, verified with a certificate authority, to decrypt the prehash code.**

Correct Answer: D

Explanation: The recipient can use the sender's public key to decrypt the prehash code, ensuring the message is authentic and unchanged, which provides assurance of confidentiality, message integrity, and nonrepudiation.

QUESTION 784

Use of asymmetric encryption in an internet e-commerce site, where there is one private key for the hosting server and the public key is widely distributed to the customers, is MOST likely to provide comfort to the:

- A) **Customer over the authenticity of the hosting organization.**
- B) Hosting organization over the authenticity of the customer.
- C) Customer over the confidentiality of messages from the hosting organization.
- D) Hosting organization over the confidentiality of messages passed to the customer.

Correct Answer: A

Explanation: The customer can be assured of the authenticity of the hosting organization because only the real site can encrypt with the private key, which the customer can decrypt with the public key.

QUESTION 785

E-mail message authenticity and confidentiality is BEST achieved by signing the message using the:

- A) **Sender's private key and encrypting the message using the receiver's public key.**
- B) Sender's public key and encrypting the message using the receiver's private key.
- C) Receiver's private key and encrypting the message using the sender's public key.
- D) Receiver's public key and encrypting the message using the sender's private key.

Correct Answer: A

Explanation: By signing with the sender's private key, the receiver can verify authenticity with the sender's public key. By encrypting the message with the receiver's public key, only the receiver can decrypt it.

QUESTION 786

An organization is considering connecting a critical PC-based system to the internet. Which of the following would provide the BEST protection against hacking?

- A) **An application-level gateway**
- B) A remote access server
- C) A proxy server
- D) Port scanning

Correct Answer: A

Explanation: An application-level gateway provides the most detailed and secure filtering by inspecting traffic at the application layer, which can protect against hacking attempts more effectively than the other options.

QUESTION 787

Which of the following is the MOST secure and economical method for connecting a private network over the Internet in a small- to medium-sized organization?

- A) **Virtual private network**

- B) Dedicated line
- C) Leased line
- D) Integrated services digital network (ISDN)

Correct Answer: A
Explanation: A Virtual Private Network (VPN) is the most secure and cost-effective solution, using encryption to secure data sent over public networks, while the other options are typically more expensive.

QUESTION 788
The potential for unauthorized system access by way of terminals or workstations within an organization's facility is increased when:

- A) **Connecting points are available in the facility to connect laptops to the network.**
- B) Users take precautions to keep their passwords confidential.
- C) Terminals with password protection are located in insecure locations.
- D) Terminals are located within the facility in small clusters under the supervision of an administrator.

Correct Answer: A
Explanation: Connecting points available in the facility can allow unauthorized individuals to connect to the network with a laptop, increasing the risk of unauthorized access.

QUESTION 789
Which of the following functions is performed by a virtual private network (VPN)?

- A) **Hiding information from sniffers on the net**
- B) Enforcing security policies
- C) Detecting misuse or mistakes
- D) Regulating access

Correct Answer: A
Explanation: A VPN encrypts traffic, hiding information from sniffers. It does not enforce policies, detect misuse, or regulate access directly, but provides secure communication.

QUESTION 790
Applying a digital signature to data traveling in a network provides:

- A) Confidentiality and integrity.
- B) Security and nonrepudiation.
- C) **Integrity and nonrepudiation.**
- D) Confidentiality and nonrepudiation.

Correct Answer: C
Explanation: A digital signature ensures integrity (the data has not been altered) and nonrepudiation (the sender cannot deny sending the message). It does not provide confidentiality, which requires encryption.

QUESTION 791
Which of the following would an IS auditor consider a weakness when performing an audit of an organization that uses a public key infrastructure (PKI) with digital certificates for its business-to-consumer transactions via the internet?

- A. Customers are widely dispersed geographically, but the certificate authorities are not.
- B. Customers can make their transactions from any computer or mobile device.
- C. The certificate authority has several data processing subcenters to administer certificates.
- D. The organization is the owner of the certificate authority.

Correct Answer: D
Explanation: If the organization is the owner of the certificate authority (CA), this could lead to a conflict of interest, potentially undermining the trustworthiness of the PKI. A CA should be a trusted third party to avoid any appearance of impropriety in generating certificates. The other options are not considered weaknesses.

QUESTION 792

Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the internet?

- A. Transport mode with authentication header (AH) plus encapsulating security payload (ESP)
- B. Secure Sockets Layer (SSL) mode
- C. Tunnel mode with AH plus ESP
- D. Triple-DES encryption mode

Correct Answer: C

Explanation: Tunnel mode with AH (Authentication Header) plus ESP (Encapsulating Security Payload) provides the greatest amount of security because it encrypts both the payload and the header, securing the entire data packet. This ensures confidentiality, integrity, and authenticity. Transport mode only protects the payload, while SSL and Triple-DES modes do not provide full protection of the packet.

QUESTION 793

Which of the following is the MOST reliable sender authentication method?

- A. Digital signatures
- B. Asymmetric cryptography
- C. Digital certificates
- D. Message authentication code (MAC)

Correct Answer: C

Explanation: Digital certificates are issued by a trusted third party (certificate authority) and provide the most reliable method for sender authentication. While digital signatures and asymmetric cryptography are also important for ensuring the authenticity of a message, digital certificates validate the sender's public key, ensuring that the sender is who they claim to be.

QUESTION 794

Which of the following provides the GREATEST assurance of message authenticity?

- A. The prehash code is derived mathematically from the message being sent.
- B. The prehash code is encrypted using the sender's private key.
- C. The prehash code and the message are encrypted using the secret key.
- D. The sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

Correct Answer: B

Explanation: Encrypting the prehash code using the sender's private key provides the greatest assurance of message authenticity. It ensures that the message was not altered and can only be verified using the sender's public key, proving the message's origin and authenticity.

QUESTION 795

Which of the following internet security threats could compromise integrity?

- A. Theft of data from the client
- B. Exposure of network configuration information
- C. A Trojan horse browser
- D. Eavesdropping on the net

Correct Answer: C

Explanation: A Trojan horse browser can compromise the integrity of data by modifying it without the user's knowledge. Other options, such as data theft and eavesdropping, primarily compromise confidentiality.

QUESTION 796

Which of the following is a concern when data are transmitted through Secure Sockets Layer (SSL) encryption, implemented on a trading partner's server?

- A. The organization does not have control over encryption.
- B. Messages are subjected to wiretapping.
- C. Data might not reach the intended recipient.

- D. The communication may not be secure.

Correct Answer: A

Explanation: The primary concern with using SSL encryption on a trading partner's server is that the organization does not have control over the encryption process. The trading partner is responsible for encryption and decryption, which introduces potential risks. Wiretapping is not a concern since SSL encrypts the communication.

QUESTION 797

If inadequate, which of the following would be the MOST likely contributor to a denial-of-service (DoS) attack?

- A. Router configuration and rules
- B. Design of the internal network
- C. Updates to the router system software
- D. Audit testing and review techniques

Correct Answer: A

Explanation: Inadequate router configuration and rules could expose the network to denial-of-service (DoS) attacks. Routers control access to the network, and poor configuration could allow malicious traffic to flood the network. The other options are less likely to directly contribute to a DoS attack.

QUESTION 798

The Secure Sockets Layer (SSL) protocol addresses the confidentiality of a message through:

- A. symmetric encryption.
- B. message authentication code.
- C. hash function.
- D. digital signature certificates.

Correct Answer: A

Explanation: SSL ensures the confidentiality of a message through symmetric encryption. It uses symmetric keys to encrypt and decrypt data exchanged between a client and server. Message authentication codes and hash functions ensure integrity, while digital signature certificates ensure authenticity.

QUESTION 799

The PRIMARY goal of a web site certificate is:

- A. authentication of the web site that will be surfed.
- B. authentication of the user who surfs through that site.
- C. preventing surfing of the web site by hackers.
- D. the same purpose as that of a digital certificate.

Correct Answer: A

Explanation: The primary goal of a website certificate is to authenticate the website, ensuring the user that they are accessing a legitimate site. It does not authenticate users or prevent hackers from accessing the site.

QUESTION 800

An IS auditor performing detailed network assessments and access control reviews should FIRST:

- A. determine the points of entry.
- B. evaluate users' access authorization.
- C. assess users' identification and authorization.
- D. evaluate the domain-controlling server configuration.

Correct Answer: A

Explanation: When conducting network assessments and access control reviews, the IS auditor should first determine the points of entry into the system. Identifying the entry points helps ensure the appropriate controls are in place to protect the network from unauthorized access. Other steps, such as evaluating access authorization and reviewing server configurations, come later.

QUESTION 801

The difference between a vulnerability assessment and a penetration test is that a vulnerability assessment:

- A. searches and checks the infrastructure to detect vulnerabilities, whereas penetration testing intends to exploit the vulnerabilities to probe the damage that could result from the vulnerabilities.
- B. and penetration tests are different names for the same activity.
- C. is executed by automated tools, whereas penetration testing is a totally manual process.
- D. is executed by commercial tools, whereas penetration testing is executed by public processes.

Correct Answer: A

Explanation: A vulnerability assessment is designed to identify and report vulnerabilities in a system without actively exploiting them, while penetration testing actively tries to exploit the vulnerabilities to determine the extent of potential damage. The two are distinct processes, with different goals and techniques, but both can be performed using automated or manual tools.

QUESTION 802

The most common problem in the operation of an intrusion detection system (IDS) is:

- A. the detection of false positives.
- B. receiving trap messages.
- C. reject-error rates.
- D. denial-of-service attacks.

Correct Answer: A

Explanation: The most common issue with IDSs is the generation of false positives, where legitimate activity is incorrectly identified as a security threat. This can lead to alert fatigue and make it harder to identify real attacks. Trap messages are part of SNMP and not specific to IDS, reject-error rates relate to biometrics, and denial-of-service attacks are a type of threat, not an operational problem for IDS.

QUESTION 803

Which of the following provides nonrepudiation services for e-commerce transactions?

- A. Public key infrastructure (PKI)
- B. Data Encryption Standard (DES)
- C. Message authentication code (MAC)
- D. Personal identification number (PIN)

Correct Answer: A

Explanation: PKI provides nonrepudiation services by using digital certificates and digital signatures, ensuring that the sender of a message cannot deny their identity. DES is a symmetric encryption algorithm, MAC provides message integrity, and a PIN verifies identity but does not ensure nonrepudiation.

QUESTION 804

While copying files from a floppy disk, a user introduced a virus into the network. Which of the following would MOST effectively detect the existence of the virus?

- A. A scan of all floppy disks before use
- B. A virus monitor on the network file server
- C. Scheduled daily scans of all network drives
- D. A virus monitor on the user's personal computer

Correct Answer: C

Explanation: Scheduled daily scans of all network drives will detect any viruses that may have been introduced into the system. Scanning all floppy disks before use or using virus monitors on personal computers or servers are preventive measures but do not guarantee detection after infection.

QUESTION 805

Which of the following message services provides the strongest evidence that a specific action has occurred?

- A. Proof of delivery
- B. Nonrepudiation

- C. Proof of submission
- D. Message origin authentication

Correct Answer: B
Explanation: Nonrepudiation provides strong evidence that a specific action occurred, typically through digital signatures. It ensures that the sender of a message cannot deny sending it, providing stronger proof than delivery or submission confirmations or message origin authentication.

QUESTION 806
The PRIMARY objective of Secure Sockets Layer (SSL) is to ensure:

- A. only the sender and receiver are able to encrypt/decrypt the data.
- B. the sender and receiver can authenticate their respective identities.
- C. the alteration of transmitted data can be detected.
- D. the ability to identify the sender by generating a one-time session key.

Correct Answer: A
Explanation: SSL's main goal is to secure communication by encrypting data between the sender and receiver, ensuring that only they can decrypt it. Although SSL supports authentication and data integrity, its primary purpose is to provide confidentiality by encrypting the transmitted data.

QUESTION 807
The role of the certificate authority (CA) as a third party is to:

- A. provide secured communication and networking services based on certificates.
- B. host a repository of certificates with the corresponding public and secret keys issued by that CA.
- C. act as a trusted intermediary between two communication partners.
- D. confirm the identity of the entity owning a certificate issued by that CA.

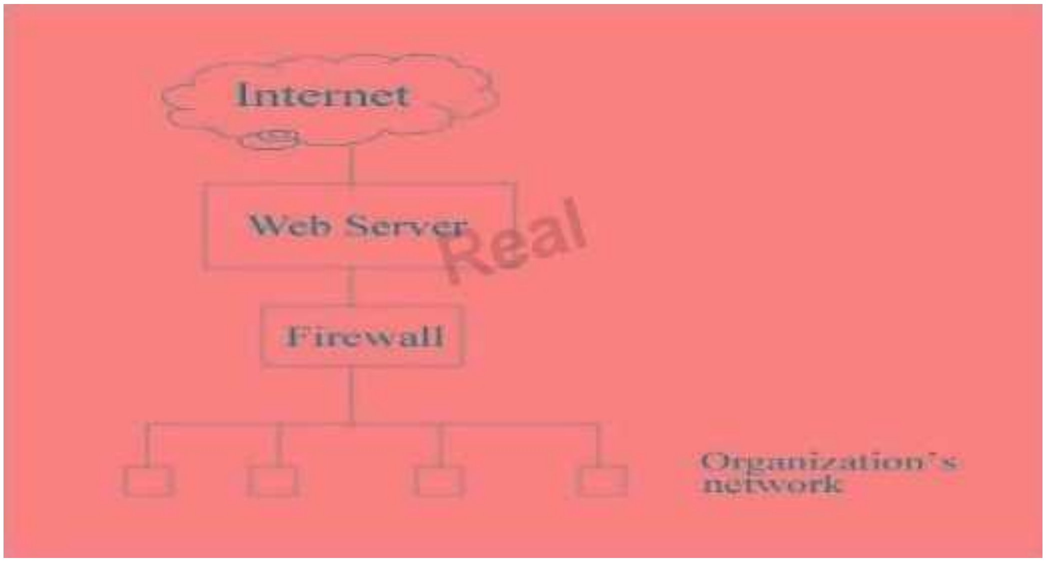
Correct Answer: D
Explanation: The primary role of a CA is to verify the identity of an entity before issuing a digital certificate. This ensures that the entity's public key is correctly associated with its identity. The CA does not provide communication services or store secret keys, and while it helps with trust, it is not involved in direct communication.

QUESTION 808
Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?

- A. The buyer is assured that neither the merchant nor any other party can misuse their credit card data.
- B. All personal SET certificates are stored securely in the buyer's computer.
- C. The buyer is liable for any transaction involving his/her personal SET certificates.
- D. The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

Correct Answer: C
Explanation: In SET, the cardholder assumes responsibility for any use of their personal SET certificates. While SET improves security for credit card transactions, the buyer is still liable for any transactions made with their certificates. The protocol does not eliminate the need to handle credit card information or guarantee that certificates are securely stored.

QUESTION 809
E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network.



The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

- A. alert the appropriate staff.
- B. create an entry in the log.
- C. close firewall-2.
- D. close firewall-1.

Correct Answer: C
Explanation: If traffic that bypasses the mail gateway is detected, firewall-1 may have been compromised. The first priority is to close firewall-2 to protect the internal network from unauthorized traffic. Closing firewall-1 might not be possible if it has already been compromised. Logging the incident or alerting staff is secondary to immediately securing the network.

QUESTION 810
An IS auditor should be MOST concerned with what aspect of an authorized honeypot?

- A. The data collected on attack methods
- B. The information offered to outsiders on the honeypot
- C. The risk that the honeypot could be used to launch further attacks on the organization's infrastructure
- D. The risk that the honeypot would be subject to a distributed denial-of-service attack

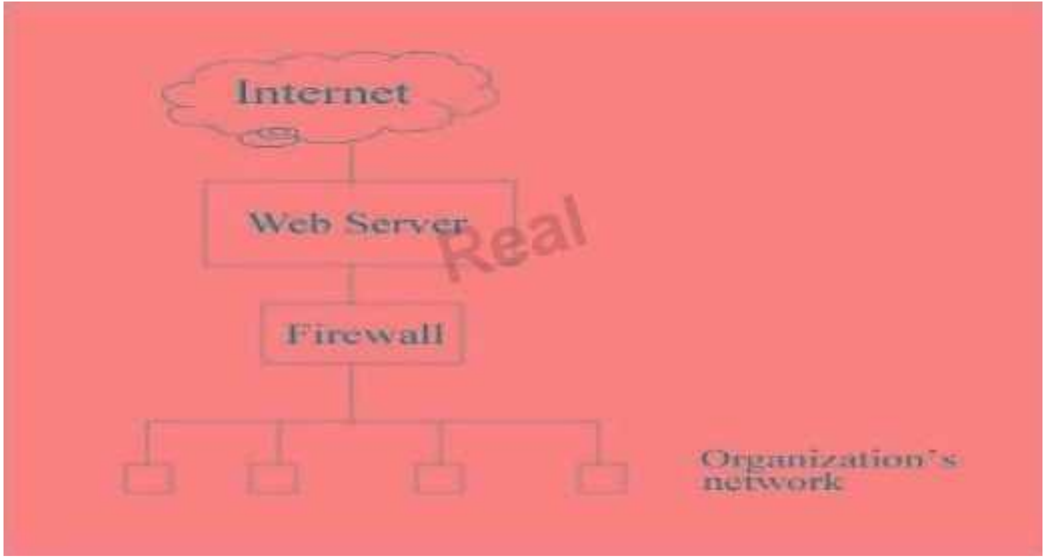
Correct Answer: C
Explanation: The primary concern is that the honeypot could be used by attackers to infiltrate the organization's systems and launch further attacks. While honeypots gather valuable information about attack methods, they can also become a liability if not properly isolated from critical infrastructure.

QUESTION 811
Which of the following should be a concern to an IS auditor reviewing a wireless network?

- A. 128-bit static-key WEP (Wired Equivalent Privacy) encryption is enabled.
- B. SSID (Service Set Identifier) broadcasting has been enabled.
- C. Antivirus software has been installed in all wireless clients.
- D. MAC (Media Access Control) access control filtering has been deployed.

Correct Answer: B
Explanation: SSID broadcasting should be disabled to prevent unauthorized users from easily discovering the wireless network. Enabling SSID broadcasting makes the network more vulnerable to unauthorized access. WEP, while not highly secure, adds some protection, and antivirus and MAC filtering strengthen security.

QUESTION 812
To detect attack attempts that the firewall is unable to recognize, an IS auditor should recommend placing a network intrusion detection system (IDS) between the:



- A. Firewall and the organization's network.
- B. Internet and the firewall.
- C. Internet and the web server.
- D. Web server and the firewall.

Correct Answer: A
Explanation: Placing a network-based IDS between the firewall and the organization's network ensures that any attacks that bypass the firewall will still be detected. This setup monitors all traffic that reaches the internal network, enhancing the ability to detect potential intrusions that the firewall may miss.

QUESTION 813
Which of the following ensures a sender's authenticity and an e-mail's confidentiality?

- A. Encrypting the hash of the message with the sender's private key and thereafter encrypting the hash of the message with the receiver's public key
- B. The sender digitally signing the message and thereafter encrypting the hash of the message with the sender's private key
- C. Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key
- D. Encrypting the message with the sender's private key and encrypting the message hash with the receiver's public key.

Correct Answer: C
Explanation: To ensure both authenticity and confidentiality, the message should be encrypted first with the sender's private key (ensuring authenticity) and then with the receiver's public key (ensuring confidentiality). This double encryption process ensures that the message remains private and that its origin is verified.

QUESTION 814

An efficient use of public key infrastructure (PKI) should encrypt the:

- A. entire message.
- B. private key.
- C. public key.
- D. symmetric session key.

Correct Answer: D

Explanation: PKI systems are computationally intensive, so they are often used to exchange symmetric session keys, which are then used to encrypt and decrypt the actual message. Symmetric encryption is faster and more efficient for bulk data encryption, while PKI handles the secure exchange of the session keys.

QUESTION 815

Which of the following cryptographic systems is MOST appropriate for bulk data encryption and small devices such as smart cards?

- A. DES
- B. AES
- C. Triple DES
- D. RSA

Correct Answer: B

Explanation: AES (Advanced Encryption Standard) is well-suited for bulk data encryption and can run efficiently on a variety of platforms, including small devices like smart cards. DES is no longer considered secure, Triple DES is slower, and RSA is more suited for encrypting small amounts of data.

QUESTION 816

Disabling which of the following would make wireless local area networks more secure against unauthorized access?

- A. MAC (Media Access Control) address filtering
- B. WPA (Wi-Fi Protected Access Protocol)
- C. LEAP (Lightweight Extensible Authentication Protocol)
- D. SSID (service set identifier) broadcasting

Correct Answer: D

Explanation: Disabling SSID broadcasting makes it harder for unauthorized users to find and access the wireless network. Enabling MAC address filtering, WPA, and LEAP enhances security, but SSID broadcasting should be turned off to add an additional layer of security by making the network less visible.

QUESTION 817

Which of the following is BEST suited for secure communications within a small group?

- A. Key distribution center
- B. Certification authority
- C. Web of trust
- D. Kerberos Authentication System

Correct Answer: C

Explanation: A web of trust is ideal for secure communications in a small group. It allows users to verify each other’s public keys through trusted relationships. In contrast, a key distribution center and certification authority are better suited for larger organizations or formal communications, while Kerberos is used to manage authentication in a larger network environment.

QUESTION 818

Which of the following is the MOST important action in recovering from a cyberattack?

- A. Creation of an incident response team
- B. Use of cyberforensic investigators
- C. Execution of a business continuity plan
- D. Filing an insurance claim

Correct Answer: C
Explanation: The execution of a business continuity plan (BCP) is crucial in recovering from a cyberattack, as it ensures that critical business functions can continue while the attack is addressed. The creation of an incident response team and the use of cyberforensics are preventive and investigative measures, but BCP is the key to minimizing the impact of the attack.

QUESTION 819
What method might an IS auditor utilize to test wireless security at branch office locations?

- **A.** War dialing
- **B.** Social engineering
- **C.** War driving
- **D.** Password cracking

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
War driving is a technique used for locating and accessing wireless networks by moving around a building with a wireless-enabled device. This helps to identify unsecured or weakly protected wireless networks. War dialing is used for gaining access to a network by dialing multiple phone numbers. Social engineering is about exploiting human weaknesses to gain access to systems. Password cracking attempts to guess users' passwords but does not specifically target wireless network security.

QUESTION 820
In a public key infrastructure, a registration authority:

- **A.** Verifies information supplied by the subject requesting a certificate.
- **B.** Issues the certificate after the required attributes are verified and the keys are generated.
- **C.** Digitally signs a message to achieve nonrepudiation of the signed message.
- **D.** Registers signed messages to protect them from future repudiation.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
A registration authority (RA) is responsible for verifying the identity and legitimacy of a requestor before a certificate is issued. The certification authority (CA), not the RA, is responsible for issuing certificates. The RA does not sign messages or register signed messages.

QUESTION 821
Confidentiality of the data transmitted in a wireless LAN is BEST protected if the session is:

- **A.** Restricted to predefined MAC addresses.
- **B.** Encrypted using static keys.
- **C.** Encrypted using dynamic keys.
- **D.** Initiated from devices that have encrypted storage.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Dynamic encryption keys, which change regularly, provide better confidentiality than static keys. Limiting access to predefined MAC addresses is not sufficient to ensure confidentiality. Static encryption keys are more vulnerable to being compromised. Encryption of device storage does not protect the data transmitted over the network.

QUESTION 822
Which of the following provides the MOST relevant information for proactively strengthening security settings?

- **A.** Bastion host
- **B.** Intrusion detection system

- **C.** Honeypot
- **D.** Intrusion prevention system

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
A honeypot is designed to lure attackers, providing valuable information about attack strategies and methods, which can be used to proactively strengthen security settings. A bastion host does not provide detailed insights into attackers' methods. Intrusion detection and prevention systems are focused on identifying and stopping attacks in progress rather than proactively gathering intelligence.

QUESTION 823
Over the long term, which of the following has the greatest potential to improve the security incident response process?

- **A.** A walkthrough review of incident response procedures
- **B.** Postevent reviews by the incident response team
- **C.** Ongoing security training for users
- **D.** Documenting responses to an incident

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Postevent reviews provide valuable insights into how incidents were handled, identifying gaps and opportunities for improvement. While walkthrough reviews, training, and documentation are important, postevent reviews have the greatest potential to improve the response process over time by learning from real-world incidents.

QUESTION 824
When reviewing an intrusion detection system (IDS), an IS auditor should be MOST concerned about which of the following?

- **A.** Number of nonthreatening events identified as threatening
- **B.** Attacks not being identified by the system
- **C.** Reports/logs being produced by an automated tool
- **D.** Legitimate traffic being blocked by the system

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The greatest concern is the failure of the IDS to identify attacks, as these could lead to significant security breaches. False positives (nonthreatening events identified as threats) are a problem but are generally known and can be managed. Legitimate traffic being blocked is not as critical as missing real attacks. Automated tools generating reports are a normal feature and not a concern.

QUESTION 825
Distributed denial-of-service (DDOS) attacks on Internet sites are typically evoked by hackers using which of the following?

- **A.** Logic bombs
- **B.** Phishing
- **C.** Spyware
- **D.** Trojan horses

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Trojan horses are malicious software that can allow attackers to take control of multiple computers. These compromised computers can then be used in a DDOS attack to flood a target website with traffic, overwhelming its

servers. Logic bombs are timed attacks, phishing aims to trick users into giving up sensitive information, and spyware collects data from an infected device but does not directly cause DDOS attacks.

QUESTION 826

Validated digital signatures in an e-mail software application will:

- **A.** Help detect spam.
- **B.** Provide confidentiality.
- **C.** Add to the workload of gateway servers.
- **D.** Significantly reduce available bandwidth.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Validated digital signatures in email help ensure that the sender is legitimate, which can aid in detecting spam or malicious emails. Digital signatures do not inherently provide confidentiality, as they do not encrypt the content. Their impact on server workload and bandwidth is minimal.

QUESTION 827

In transport mode, the use of the Encapsulating Security Payload (ESP) protocol is advantageous over the Authentication Header (AH) protocol because it provides:

- **A.** Connectionless integrity.
- **B.** Data origin authentication.
- **C.** Antireplay service.
- **D.** Confidentiality.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
ESP provides confidentiality by encrypting the payload of the communication, which AH does not do. Both ESP and AH offer connectionless integrity, data origin authentication, and antireplay services, but ESP additionally provides encryption for confidentiality.

QUESTION 828

An IS auditor notes that IDS log entries related to port scanning are not being analyzed. This lack of analysis will MOST likely increase the risk of success of which of the following attacks?

- **A.** Denial-of-service
- **B.** Replay
- **C.** Social engineering
- **D.** Buffer overflow

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Port scanning is often used as a precursor to a denial-of-service (DoS) attack. By identifying open ports and vulnerabilities, attackers can launch DoS attacks. A replay attack involves re-sending captured data, social engineering targets human vulnerabilities, and buffer overflow exploits flaws in code.

QUESTION 829

IS management recently replaced its existing wired local area network (LAN) with a wireless infrastructure to accommodate the increased use of mobile devices within the organization. This will increase the risk of which of the following attacks?

- **A.** Port scanning
- **B.** Back door
- **C.** Man-in-the-middle
- **D.** War driving

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
War driving involves scanning for wireless networks, often by moving around with a device that can detect wireless signals. This attack becomes a greater risk with a wireless LAN infrastructure. Port scanning is more common with wired networks, back doors are vulnerabilities in software, and man-in-the-middle attacks are a different type of network interception.

QUESTION 830
Which of the following encryption techniques will BEST protect a wireless network from a man-in-the-middle attack?

- **A.** 128-bit wired equivalent privacy (WEP)
- **B.** MAC-based pre-shared key (PSK)
- **C.** Randomly generated pre-shared key (PSK)
- **D.** Alphanumeric service set identifier (SSID)

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
A randomly generated pre-shared key (PSK) offers stronger protection because it is difficult to predict and less susceptible to brute-force attacks. WEP has known weaknesses, and using a MAC-based PSK is less secure because MAC addresses can be spoofed. The SSID is not a security measure, as it is often broadcast in plaintext.

QUESTION 831
The IS management of a multinational company is considering upgrading its existing virtual private network (VPN) to support voice-over IP (VoIP) communications via tunneling. Which of the following considerations should be PRIMARILY addressed?

- **A.** Reliability and quality of service (QoS)
- **B.** Means of authentication
- **C.** Privacy of voice transmissions
- **D.** Confidentiality of data transmissions

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
While the existing VPN likely handles authentication and confidentiality through tunneling, the primary consideration when implementing VoIP is the reliability and quality of service (QoS). VoIP requires low latency and consistent delivery of packets, which makes QoS a crucial concern. Privacy and confidentiality are typically addressed by the VPN protocols already in place.

QUESTION 832
Which of the following antispam filtering techniques would BEST prevent a valid, variable-length email message containing a heavily weighted spam keyword from being labeled as spam?

- **A.** Heuristic (rule-based)
- **B.** Signature-based
- **C.** Pattern matching
- **D.** Bayesian (statistical)

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Bayesian filtering applies statistical modeling to messages by performing a frequency analysis on each word and evaluating the message as a whole. It can ignore suspicious keywords if the overall content appears legitimate.

Heuristic filtering might require additional rules for new exceptions, and signature-based filtering fails with variable-length messages. Pattern matching is a less effective rule-based method that operates at the word level.

QUESTION 833
Which of the following public key infrastructure (PKI) elements provides detailed descriptions for dealing with a compromised private key?

- **A.** Certificate revocation list (CRL)
- **B.** Certification practice statement (CPS)
- **C.** Certificate policy (CP)
- **D.** PKI disclosure statement (PDS)

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The Certification Practice Statement (CPS) provides instructions on handling key compromises. The Certificate Revocation List (CRL) simply lists revoked certificates. The Certificate Policy (CP) sets general requirements, and the PKI Disclosure Statement (PDS) outlines legal responsibilities.

QUESTION 834
Active radio frequency ID (RFID) tags are subject to which of the following exposures?

- **A.** Session hijacking
- **B.** Eavesdropping
- **C.** Malicious code
- **D.** Phishing

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Like other wireless devices, active RFID tags can be subject to eavesdropping. They transmit signals that can be intercepted, but they are not directly vulnerable to session hijacking, malicious code, or phishing attacks.

QUESTION 835
When conducting a penetration test of an organization's internal network, which of the following approaches would BEST enable the conductor of the test to remain undetected on the network?

- **A.** Use the IP address of an existing file server or domain controller.
- **B.** Pause the scanning every few minutes to allow thresholds to reset.
- **C.** Conduct the scans during evening hours when no one is logged in.
- **D.** Use multiple scanning tools since each tool has different characteristics.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Pausing scans helps avoid exceeding traffic thresholds that might trigger alerts. Using the IP address of an existing server risks detection due to address conflicts, scanning during off-hours increases chances of detection, and multiple scanning tools could trigger alerts more easily.

QUESTION 836
Two-factor authentication can be circumvented through which of the following attacks?

- **A.** Denial-of-service
- **B.** Man-in-the-middle
- **C.** Keylogging
- **D.** Brute force

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:

A man-in-the-middle attack intercepts communication between the user and the system, enabling the attacker to capture authentication details. Keylogging and brute force attacks can compromise single-factor authentication but are less effective against two-factor authentication.

QUESTION 837

An organization can ensure that the recipients of emails from its employees can authenticate the identity of the sender by:

- **A.** Digitally signing all email messages.
- **B.** Encrypting all email messages.
- **C.** Compressing all email messages.
- **D.** Password-protecting all email messages.

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Digital signatures ensure that the recipient can verify the sender's identity. Encryption ensures confidentiality but does not authenticate the sender. Compressing and password-protecting messages do not provide authentication.

QUESTION 838

Sending a message and a message hash encrypted by the sender's private key will ensure:

- **A.** Authenticity and integrity.
- **B.** Authenticity and privacy.
- **C.** Integrity and privacy.
- **D.** Privacy and nonrepudiation.

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Encrypting the message and hash with the sender's private key ensures authenticity (proving the sender's identity) and integrity (the message was not altered). Encrypting with the sender's private key alone does not ensure privacy because anyone with the sender's public key can decrypt the message.

QUESTION 839

Which of the following is a passive attack on a network?

- **A.** Message modification
- **B.** Masquerading
- **C.** Denial-of-service
- **D.** Traffic analysis

Correct Answer: D

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Traffic analysis is a passive attack where the attacker observes and analyzes the communication patterns between network devices. Message modification, masquerading, and denial-of-service are active attacks, as they involve directly altering or interfering with the communication.

QUESTION 840

An organization has a mix of access points that cannot be upgraded to stronger security and newer access points having advanced wireless security. An IS auditor recommends replacing the nonupgradeable access points. Which of the following would BEST justify the IS auditor's recommendation?

- **A.** The new access points with stronger security are affordable.
- **B.** The old access points are poorer in terms of performance.
- **C.** The organization's security would be as strong as its weakest points.
- **D.** The new access points are easier to manage.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The organization's security is compromised by the weakest access points, making it vulnerable to attacks. Affordability, performance, and manageability are secondary to the security risks posed by the old access points.

QUESTION 841
An investment advisor e-mails periodic newsletters to clients and wants reasonable assurance that no one has modified the newsletter. This objective can be achieved by:

- encrypting the hash of the newsletter using the advisor's private key.
- encrypting the hash of the newsletter using the advisor's public key.
- digitally signing the document using the advisor's private key.
- encrypting the newsletter using the advisor's private key.

Correct Answer: A
Explanation: The objective is to assure recipients that the newsletter has not been modified (message integrity). By encrypting the hash of the newsletter using the advisor's private key, recipients can decrypt it with the public key to verify that the newsletter is unaltered. Encrypting the newsletter using a private key would not be appropriate, as it would also involve confidentiality, which is not the main concern in this case.

QUESTION 842
An IS auditor reviewing wireless network security determines that the Dynamic Host Configuration Protocol (DHCP) is disabled at all wireless access points. This practice:

- reduces the risk of unauthorized access to the network.
- is not suitable for small networks.
- automatically provides an IP address to anyone.
- increases the risks associated with Wireless Encryption Protocol (WEP).

Correct Answer: A
Explanation: Disabling DHCP reduces the risk of unauthorized access by requiring devices to use static IP addresses. This makes it harder for unauthorized devices to connect. DHCP is suitable for small networks, and its absence means IP addresses are not automatically assigned, reducing certain risks. Disabling DHCP does not increase the risks associated with WEP.

QUESTION 843
A virtual private network (VPN) provides data confidentiality by using:

- Secure Sockets Layer (SSL)
- Tunneling
- Digital signatures
- Phishing

Correct Answer: B
Explanation: VPNs provide data confidentiality by encapsulating and encrypting data through a process called tunneling. SSL is used for securing browser-server communication, digital signatures are used for authentication, and phishing is a social engineering attack, not related to VPNs.

QUESTION 844
In auditing a web server, an IS auditor should be concerned about the risk of individuals gaining unauthorized access to confidential information through:

- common gateway interface (CGI) scripts.
- enterprise Java beans (EJBs).
- applets.
- web services.

Correct Answer: A

Explanation: CGI scripts are executable programs that run on the server, which can introduce vulnerabilities. Bugs in CGI scripts may allow unauthorized access to the server, potentially compromising confidential data. Applets, EJBs, and web services have different security considerations but are controlled differently than CGI scripts.

QUESTION 845

An IS auditor reviewing access controls for a client-server environment should FIRST:

- evaluate the encryption technique.
- identify the network access points.
- review the identity management system.
- review the application-level access controls.

Correct Answer: B

Explanation: In a client-server environment, identifying network access points is crucial as they represent potential vulnerabilities. Encryption techniques, identity management, and application-level access controls should be reviewed later, but securing network access points is the priority.

QUESTION 846

To prevent IP spoofing attacks, a firewall should be configured to drop a packet if:

- the source routing field is enabled.
- it has a broadcast address in the destination field.
- a reset flag (RST) is turned on for the TCP connection.
- dynamic routing is used instead of static routing.

Correct Answer: A

Explanation: IP spoofing attacks exploit the source-routing option in the IP protocol, allowing an attacker to insert a false source IP address. A firewall should drop packets with this option enabled to prevent such attacks. The other options are unrelated to IP spoofing.

QUESTION 847

An IS auditor reviewing the implementation of an intrusion detection system (IDS) should be MOST concerned if:

- IDS sensors are placed outside of the firewall.
- a behavior-based IDS is causing many false alarms.
- a signature-based IDS is weak against new types of attacks.
- the IDS is used to detect encrypted traffic.

Correct Answer: D

Explanation: An IDS cannot detect attacks within encrypted traffic. While false alarms and weaknesses in signature-based systems are common, the primary concern is if the IDS is expected to detect threats in encrypted communications, as it is not designed for this purpose.

QUESTION 848

Which of the following BEST describes the role of a directory server in a public key infrastructure (PKI)?

- Encrypts the information transmitted over the network
- Makes other users' certificates available to applications
- Facilitates the implementation of a password policy
- Stores certificate revocation lists (CRLs)

Correct Answer: B

Explanation: A directory server in a PKI is primarily responsible for making users' certificates available to applications. Encryption of data and storage of certificate revocation lists are roles of a security server, while password policies are not part of PKI.

QUESTION 849

An organization is using symmetric encryption. Which of the following would be a valid reason for moving to asymmetric encryption? Symmetric encryption:

- provides authenticity.

- is faster than asymmetric encryption.
- can cause key management to be difficult.
- requires a relatively simple algorithm.

Correct Answer: C

Explanation: Symmetric encryption can complicate key management since each pair of users needs a unique key. This issue is resolved in asymmetric encryption. Symmetric encryption does not provide authenticity and is generally faster but more challenging to manage due to the number of keys involved.

QUESTION 850

Which of the following would provide the BEST protection against the hacking of a computer connected to the Internet?

- A remote access server
- A proxy server
- A personal firewall
- A password-generating token

Correct Answer: C

Explanation: A personal firewall provides the best protection against hacking by filtering network traffic based on rules. While remote access servers, proxy servers, and password tokens have their uses, they do not provide the same level of direct protection against hacking attempts.

QUESTION 851

When installing an intrusion detection system (IDS), which of the following is MOST important?

- Properly locating it in the network architecture
- Preventing denial-of-service (DoS) attacks
- Identifying messages that need to be quarantined
- Minimizing the rejection errors

Correct Answer: A

Explanation: Proper placement of an IDS in the network is critical to ensure that it can monitor the right areas. A poorly positioned IDS might leave key network segments unprotected. Other factors like DoS prevention, message identification, and minimizing errors are secondary concerns to proper placement.

QUESTION 852

In a public key infrastructure (PKI), which of the following may be relied upon to prove that an online transaction was authorized by a specific customer?

- Nonrepudiation
- Encryption
- Authentication
- Integrity

Correct Answer: A

Explanation:

Nonrepudiation, achieved through the use of digital signatures, ensures that the sender of a message cannot later deny having sent it, providing proof that an online transaction was authorized by the customer. Encryption protects data, but does not prove authorization. Authentication establishes identity, and integrity ensures accuracy, but neither provides nonrepudiation.

QUESTION 853

Which of the following ensures confidentiality of information sent over the Internet?

- Digital signature
- Digital certificate
- Online Certificate Status Protocol
- Private key cryptosystem

Correct Answer: D

Explanation:

A private key cryptosystem ensures confidentiality by encrypting information sent over the Internet. Digital signatures assure data integrity, authentication, and nonrepudiation, but not confidentiality. A digital certificate binds a public key with an identity, but does not address confidentiality. Online Certificate Status Protocol (OCSP) checks the revocation status of a digital certificate.

QUESTION 854

To protect a VoIP infrastructure against a denial-of-service (DoS) attack, it is MOST important to secure the:

- Access control servers
- Session border controllers
- Backbone gateways
- Intrusion detection system (IDS)

Correct Answer: B

Explanation:

Session border controllers enhance security by hiding user addresses and controlling the access and bandwidth of VoIP traffic. They are crucial in preventing DoS attacks. While access control servers, backbone gateways, and IDSs also play roles in security, session border controllers directly mitigate DoS attack risks.

QUESTION 855

Which of the following attacks targets the Secure Sockets Layer (SSL)?

- Man-in-the-middle
- Dictionary
- Password sniffing
- Phishing

Correct Answer: A

Explanation:

A man-in-the-middle attack involves an attacker intercepting SSL traffic between the user and the server, compromising secure communication. Dictionary attacks aim to crack passwords, and phishing attacks target users rather than SSL. Password sniffing does not affect SSL because SSL traffic is encrypted.

QUESTION 856

Which of the following potentially blocks hacking attempts?

- Intrusion detection system
- Honeypot system
- Intrusion prevention system
- Network security scanner

Correct Answer: C

Explanation:

An intrusion prevention system (IPS) actively detects and blocks hacking attempts, as it is deployed in-line. An intrusion detection system (IDS) only detects attacks but does not prevent them. A honeypot lures attackers to a fake target, and a network security scanner identifies vulnerabilities without stopping them.

QUESTION 857

A web server is attacked and compromised. Which of the following should be performed FIRST to handle the incident?

- Dump the volatile storage data to a disk
- Run the server in a fail-safe mode
- Disconnect the web server from the network
- Shut down the web server

Correct Answer: C

Explanation:

The first action should be to disconnect the compromised server from the network to contain the attack and prevent further damage. Dumping volatile storage data and shutting down the server can be part of the investigation process but may cause loss of valuable information. Running the server in fail-safe mode may still allow the attack to continue.

QUESTION 858

To address a maintenance problem, a vendor needs remote access to a critical network. The MOST secure and effective solution is to provide the vendor with a:

- Secure Shell (SSH-2) tunnel for the duration of the problem
- Two-factor authentication mechanism for network access
- Dial-in access
- Virtual private network (VPN) account for the duration of the vendor support contract

Correct Answer: A

Explanation:

A Secure Shell (SSH-2) tunnel provides secure, temporary access for the vendor while minimizing the risk of unauthorized access. Two-factor authentication and VPN would provide broader access, which may be unnecessary. Dial-in access is less secure and more difficult to monitor than SSH-2.

QUESTION 859

What is the BEST approach to mitigate the risk of a phishing attack?

- Implement an intrusion detection system (IDS)
- Assess website security
- Strong authentication
- User education

Correct Answer: D

Explanation:

Phishing primarily exploits users by tricking them into divulging sensitive information. Educating users on how to recognize and avoid phishing attacks is the most effective mitigation. An IDS can detect attacks, but not all phishing attacks target systems directly. Website security and strong authentication can help, but user awareness is the best defense.

QUESTION 860

A sender of an e-mail message applies a digital signature to the digest of the message. This action provides assurance of the:

- Date and time stamp of the message
- Identity of the originating computer
- Confidentiality of the message's content
- Authenticity of the sender

Correct Answer: D

Explanation:

A digital signature verifies the authenticity of the sender by binding the sender's identity to the message. It does not provide the date or time stamp, identity of the originating computer, or ensure confidentiality, as the message content itself is not encrypted.

QUESTION 861

The BEST filter rule for protecting a network from being used as an amplifier in a denial-of-service (DoS) attack is to deny all:

- Outgoing traffic with IP source addresses external to the network
- Incoming traffic with discernible spoofed IP source addresses
- Incoming traffic with IP options set
- Incoming traffic to critical hosts

Correct Answer: A

Explanation:

By denying outgoing traffic with an external IP source address, you prevent the network from being used in DoS attacks where attackers spoof the source address to make it appear as though the attack is coming from within the network. Other options do not specifically address this issue.

QUESTION 862

The network of an organization has been the victim of several intruders' attacks. Which of the following measures would allow for the early detection of such incidents?

- Antivirus software
- Hardening the servers
- Screening routers
- Honeypots

Correct Answer: D

Explanation:

Honeypots are designed to attract and capture the attention of intruders, allowing administrators to gather data on attack trends and techniques. Since they are isolated and serve no legitimate business function, any activity directed toward them is considered suspicious, making them useful for early detection of attacks. Other options do not provide direct indications of potential attacks.

QUESTION 863

A company has decided to implement an electronic signature scheme based on public key infrastructure. The user's private key will be stored on the computer's hard drive and protected by a password. The MOST significant risk of this approach is:

- Use of the user's electronic signature by another person if the password is compromised.
- Forgery by using another user's private key to sign a message with an electronic signature.
- Impersonation of a user by substitution of the user's public key with another person's public key.
- Forgery by substitution of another person's private key on the computer.

Correct Answer: A

Explanation:

If the password protecting the user's private key is compromised, an attacker could use the user's electronic signature, representing a significant risk. Other options involve more complex scenarios that are less likely to occur.

QUESTION 864

An IS auditor selects a server for a penetration test that will be carried out by a technical specialist. Which of the following is MOST important?

- The tools used to conduct the test
- Certifications held by the IS auditor
- Permission from the data owner of the server
- An intrusion detection system (IDS) is enabled

Correct Answer: C

Explanation:

Obtaining permission from the data owner is crucial to ensure that the penetration test is authorized and that the risks are understood. Other choices, while important, do not supersede the necessity of permission from the data owner.

QUESTION 865

After observing suspicious activities in a server, a manager requests a forensic analysis. Which of the following findings should be of MOST concern to the investigator?

- Server is a member of a workgroup and not part of the server domain
- Guest account is enabled on the server
- Recently, 100 users were created in the server
- Audit logs are not enabled for the server

Correct Answer: D

Explanation:

Audit logs are essential for conducting forensic investigations as they provide evidence of activities and can help trace the steps of an attacker. The other findings, while concerning, do not directly impact the ability to conduct a thorough investigation.

QUESTION 866

Which of the following would be the GREATEST cause for concern when data are sent over the Internet using HTTPS protocol?

- Presence of spyware in one of the ends
- The use of a traffic sniffing tool
- The implementation of an RSA-compliant solution
- A symmetric cryptography is used for transmitting data

Correct Answer: A

Explanation:

Spyware on an end-user's device can capture data before it is encrypted by HTTPS, making it the greatest risk. Other options pertain to encryption techniques that are generally secure against interception.

QUESTION 867

A firewall is being deployed at a new location. Which of the following is the MOST important factor in ensuring a successful deployment?

- Reviewing logs frequently
- Testing and validating the rules
- Training a local administrator at the new location
- Sharing firewall administrative duties

Correct Answer: B

Explanation:

Testing and validating the rules before deployment is critical to ensure that the firewall is secure. Incorrect rules can lead to vulnerabilities. Other actions are also important but do not have the same immediate impact on security during deployment.

QUESTION 868

The human resources (HR) department has developed a system to allow employees to enroll in benefits via a web site on the corporate Intranet. Which of the following would protect the confidentiality of the data?

- SSL encryption
- Two-factor authentication
- Encrypted session cookies
- IP address verification

Correct Answer: A

Explanation:

SSL encryption is essential for protecting the confidentiality of data transmitted over the Internet. While the other options help with security, they do not specifically address data confidentiality during transmission.

QUESTION 869

What is the MOST prevalent security risk when an organization implements remote virtual private network (VPN) access to its network?

- Malicious code could be spread across the network
- VPN logon could be spoofed
- Traffic could be sniffed and decrypted
- VPN gateway could be compromised

Correct Answer: A

Explanation:

The most significant risk is the spread of malicious code from remote clients to the organization's network. Although other options are valid concerns, mature VPN technology effectively mitigates these risks.

QUESTION 870

The use of digital signatures:

- Requires the use of a one-time password generator.
- Provides encryption to a message.
- Validates the source of a message.
- Ensures message confidentiality.

Correct Answer: C

Explanation:

Digital signatures serve to validate the identity of the sender, ensuring the integrity and authenticity of the message. They do not inherently encrypt the message or ensure confidentiality.

QUESTION 871

The FIRST step in a successful attack to a system would be:

- Gathering information.
- Gaining access.
- Denying services.
- Evading detection.

Correct Answer: A

Explanation:

The initial phase of a successful attack involves gathering information about the target to identify vulnerabilities, making it the most critical step in the attack process.

QUESTION 872

The sender of a public key would be authenticated by a:

- Certificate authority.
- Digital signature.
- Digital certificate.
- Registration authority.

Correct Answer: C

Explanation:

A digital certificate authenticates the sender of a public key, indicating that the key holder is who they claim to be. The certificate authority issues these certificates, while digital signatures ensure message integrity.

QUESTION 873

An IS auditor finds that conference rooms have active network ports. Which of the following is MOST important to ensure?

- The corporate network is using an intrusion prevention system (IPS)
- This part of the network is isolated from the corporate network
- A single sign-on has been implemented in the corporate network
- Antivirus software is in place to protect the corporate network

Correct Answer: B

Explanation:

Isolating the conference room network from the corporate network is vital to prevent unauthorized access. An IPS and other measures are important, but isolating networks is a primary security concern.

QUESTION 874

What is the BEST action to prevent loss of data integrity or confidentiality in the case of an e-commerce application running on a LAN, processing electronic fund transfers (EFT) and orders?

- Using virtual private network (VPN) tunnels for data transfer
- Enabling data encryption within the application
- Auditing the access control to the network
- Logging all changes to access lists

Correct Answer: A

Explanation:

Using VPN tunnels for data transfer provides strong encryption, protecting both confidentiality and integrity during communication over the network. Other options are beneficial practices but do not directly provide the same level of protection during transmission.

QUESTION 875

When conducting a penetration test of an IT system, an organization should be MOST concerned with:

- The confidentiality of the report.
- Finding all possible weaknesses on the system.
- Restoring all systems to the original state.
- Logging all changes made to the production system.

Correct Answer: C

Explanation:

The ability to restore all systems to their original state after a penetration test is paramount to ensure business continuity and security. While the other items are important, they are secondary to the need for restoration.

QUESTION 876

Which of the following penetration tests would MOST effectively evaluate incident handling and response capabilities of an organization?

- Targeted testing
- External testing
- Internal testing
- Double-blind testing

  Correct Answer: D

  Explanation:

  In a double-blind test, both the administrator and security staff are unaware of the test, allowing for a realistic assessment of the organization's incident handling and response capabilities. Other testing types involve prior notification, which may skew the results.

QUESTION 877

When protecting an organization's IT systems, which of the following is normally the next line of defense after the network firewall has been compromised?

- Personal firewall
- Antivirus programs
- Intrusion detection system (IDS)
- Virtual local area network (VLAN) configuration

  Correct Answer: C

  Explanation:

  An Intrusion Detection System (IDS) is crucial after a firewall compromise, as it can detect abnormal activities and help identify and respond to security incidents.

QUESTION 878

In wireless communication, which of the following controls allows the device receiving the communications to verify that the received communications have not been altered in transit?

- Device authentication and data origin authentication
- Wireless intrusion detection (IDS) and prevention systems (IPS)
- The use of cryptographic hashes
- Packet headers and trailers

Correct Answer: C

Explanation:

Cryptographic hashes enable verification that data has not been altered during transmission. This method effectively prevents message modification attacks, ensuring data integrity.

QUESTION 879

An organization is planning to replace its wired networks with wireless networks. Which of the following would BEST secure the wireless network from unauthorized access?

- Implement Wired Equivalent Privacy (WEP)
- Permit access to only authorized Media Access Control (MAC) addresses
- Disable open broadcast of service set identifiers (SSID)
- Implement Wi-Fi Protected Access (WPA) 2

Correct Answer: D

Explanation:

Wi-Fi Protected Access (WPA) 2 provides robust security through the Advanced Encryption Standard (AES), making it the best option for securing a wireless network. Other methods, such as WEP, are outdated and vulnerable.

QUESTION 880

An IS auditor is reviewing a software-based firewall configuration. Which of the following represents the GREATEST vulnerability? The firewall software:

- Is configured with an implicit deny rule as the last rule in the rule base.
- Is installed on an operating system with default settings.
- Has been configured with rules permitting or denying access to systems or networks.
- Is configured as a virtual private network (VPN) endpoint.

Correct Answer: B

Explanation:

Using default settings poses significant risks as they are well-known and can be easily exploited by attackers. A hardened operating system is crucial for firewall security.

QUESTION 881

The GREATEST risk posed by an improperly implemented intrusion prevention system (IPS) is:

- That there will be too many alerts for system administrators to verify.
- Decreased network performance due to IPS traffic.
- The blocking of critical systems or services due to false triggers.
- Reliance on specialized expertise within the IT organization.

Correct Answer: C

Explanation:

The most significant risk is the possibility of false triggers that may block critical systems or services, potentially leading to disruptions in business operations.

QUESTION 882

The MOST effective control for reducing the risk related to phishing is:

- Centralized monitoring of systems.

- Including signatures for phishing in antivirus software.
- Publishing the policy on antiphishing on the intranet.
- Security training for all users.

Correct Answer: D

Explanation:

Security training for users is the most effective measure against phishing, as it helps employees recognize and avoid social engineering attacks.

QUESTION 883

When reviewing a digital certificate verification process, which of the following findings represents the MOST significant risk?

- There is no registration authority (RA) for reporting key compromises.
- The certificate revocation list (CRL) is not current.
- Digital certificates contain a public key that is used to encrypt messages and verify digital signatures.
- Subscribers report key compromises to the certificate authority (CA).

Correct Answer: B

Explanation:

An outdated certificate revocation list (CRL) poses a significant risk, as it may allow the use of compromised certificates that have not been revoked.

QUESTION 884

When using a digital signature, the message digest is computed:

- Only by the sender.
- Only by the receiver.
- By both the sender and the receiver.
- By the certificate authority (CA).

Correct Answer: C

Explanation:

Both the sender and the receiver compute the message digest to verify the integrity of the message, ensuring that it has not been altered during transmission.

QUESTION 885

Which of the following would effectively verify the originator of a transaction?

- Using a secret password between the originator and the receiver
- Encrypting the transaction with the receiver's public key
- Using a portable document format (PDF) to encapsulate transaction content
- Digitally signing the transaction with the source's private key

Correct Answer: D

Explanation:

Digitally signing the transaction with the source's private key provides authentication of the originator and ensures the integrity of the transaction content.

QUESTION 886

A perpetrator looking to gain access to and gather information about encrypted data being transmitted over the network would use:

- Eavesdropping.
- Spoofing.
- Traffic analysis.
- Masquerading.

Correct Answer: C

Explanation:

Traffic analysis involves observing the patterns and characteristics of encrypted data transmissions, allowing an attacker to infer information without decrypting the data itself.

QUESTION 887

Upon receipt of the initial signed digital certificate, the user will decrypt the certificate with the public key of the:

- Registration authority (RA).
- Certificate authority (CA).
- Certificate repository.
- Receiver.

Correct Answer: B

Explanation:

The user decrypts the digital certificate using the public key of the Certificate Authority (CA), which signed the certificate to verify its authenticity.

QUESTION 888

IS management is considering a Voice-over Internet Protocol (VoIP) network to reduce telecommunication costs and management asked the IS auditor to comment on appropriate security controls. Which of the following security measures is MOST appropriate?

- Review and, where necessary, upgrade firewall capabilities
- Install modems to allow remote maintenance support access
- Create a physically distinct network to handle VoIP traffic
- Redirect all VoIP traffic to allow clear text logging of authentication credentials

Correct Answer: A

Explanation:

Reviewing and upgrading firewall capabilities is crucial to ensure that firewalls can adequately handle VoIP traffic and protect against associated vulnerabilities.

QUESTION 889

Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?

- Statistical-based
- Signature-based
- Neural network
- Host-based

Correct Answer: A

Explanation:

Statistical-based IDSs, which rely on defined norms of expected behavior, are prone to flagging normal activities as suspicious, leading to false alarms.

QUESTION 890

When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

- Hardware is protected against power surges.
- Integrity is maintained if the main power is interrupted.
- Immediate power will be available if the main power is lost.
- Hardware is protected against long-term power fluctuations.

Correct Answer: A

Explanation:

A voltage regulator protects hardware against short-term power surges, helping to prevent damage from sudden fluctuations in power supply.

QUESTION 891

Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?

- Halon gas
- Wet-pipe sprinklers
- Dry-pipe sprinklers
- Carbon dioxide gas

Correct Answer: C

Explanation:

Water sprinklers with an automatic power shutoff system are efficient and environmentally friendly. Dry-pipe sprinklers prevent leakage risks, while Halon is effective but environmentally damaging. Carbon dioxide is less efficient for occupied areas due to safety concerns.

QUESTION 892

Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

- Power line conditioners
- Surge protective devices
- Alternative power supplies
- Interruptible power supplies

Correct Answer: A

Explanation:

Power line conditioners manage voltage fluctuations and protect equipment from peaks and valleys in power supply. Other options serve different purposes, like protecting against surges or providing backup power for longer durations.

QUESTION 893

An IS auditor inspected a windowless room containing phone switching and networking equipment and documentation binders. The room was equipped with two handheld fire extinguishers—one filled with CO2, the other filled with halon. Which of the following should be given the HIGHEST priority in the auditor's report?

- The halon extinguisher should be removed because halon has a negative impact on the atmospheric ozone layer.
- Both fire suppression systems present a risk of suffocation when used in a closed room.
- The CO2 extinguisher should be removed because CO2 is ineffective for suppressing fires involving solid combustibles (paper).
- The documentation binders should be removed from the equipment room to reduce potential risks.

Correct Answer: B

Explanation:

Protecting lives is the top priority in fire suppression. Both CO2 and halon reduce oxygen levels and can pose suffocation risks in closed spaces. While halon may be environmentally harmful, the immediate concern is personal safety.

QUESTION 894

Which of the following would be BEST prevented by a raised floor in the computer machine room?

- Damage of wires around computers and servers
- A power failure from static electricity
- Shocks from earthquakes
- Water flood damage

Correct Answer: A

Explanation:

A raised floor allows for cable management, reducing the risk of damage caused by improperly placed cables. It does not effectively prevent static electricity, earthquakes, or water damage from overhead sources.

QUESTION 895

A penetration test performed as part of evaluating network security:

- Provides assurance that all vulnerabilities are discovered.
- Should be performed without warning the organization's management.
- Exploits the existing vulnerabilities to gain unauthorized access.
- Would not damage the information assets when performed at network perimeters.

Correct Answer: C

Explanation:

Penetration tests actively seek to exploit vulnerabilities to assess security measures, simulating a real attack. They can potentially damage information assets and do not guarantee all vulnerabilities will be found.

QUESTION 896

Users are issued security tokens to be used in combination with a PIN to access the corporate virtual private network (VPN). Regarding the PIN, what is the MOST important rule to be included in a security policy?

- Users should not leave tokens where they could be stolen.
- Users must never keep the token in the same bag as their laptop computer.
- Users should select a PIN that is completely random, with no repeating digits.
- Users should never write down their PIN.

Correct Answer: D

Explanation:

Writing down a PIN poses a security risk if the token is stolen. The effectiveness of two-factor authentication relies on both components being kept secret, regardless of whether the PIN is random.

QUESTION 897

Which of the following fire suppression systems is MOST appropriate to use in a data center environment?

- Wet-pipe sprinkler system
- Dry-pipe sprinkler system
- FM-200 system
- Carbon dioxide-based fire extinguishers

Correct Answer: C

Explanation:

FM-200 is a clean agent effective for gaseous fire suppression, making it suitable for sensitive equipment. Water-based extinguishers can cause damage, and carbon dioxide may not provide rapid enough protection.

QUESTION 898

During the review of a biometrics system operation, an IS auditor should FIRST review the stage of:

- Enrollment.
- Identification.
- Verification.
- Storage.

Correct Answer: A

Explanation:

Enrollment is the first step in biometric systems, where user characteristics are captured and converted into a template for future identification and verification.

QUESTION 899

An accuracy measure for a biometric system is:

- System response time.
- Registration time.
- Input file size.
- False-acceptance rate.

  Correct Answer: D

  Explanation:

  The false-acceptance rate (FAR) is a critical measure of accuracy in biometric systems, indicating how often unauthorized users are incorrectly accepted.

QUESTION 900

What is a risk associated with attempting to control physical access to sensitive areas such as computer rooms using card keys or locks?

- Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.
- The contingency plan for the organization cannot effectively test controlled access practices.
- Access cards, keys, and pads can be easily duplicated allowing easy compromise of the control.
- Removing access for those who are no longer authorized is complex.

  Correct Answer: A

  Explanation:

  Piggybacking, where unauthorized individuals follow authorized personnel into restricted areas, poses a significant security risk in physical access control.

QUESTION 901

An organization with extremely high security requirements is evaluating the effectiveness of biometric systems. Which of the following performance indicators is MOST important?

- False-acceptance rate (FAR)
- Equal-error rate (EER)
- False-rejection rate (FRR)
- False-identification rate (FIR)

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

FAR is the frequency of accepting an unauthorized person as authorized, thereby granting access when it should be denied. In an organization with high security requirements, user annoyance with a higher FRR is less important, since it is better to deny access to an authorized individual than to grant access to an unauthorized individual. EER is the point where the FAR equals the FRR; therefore, it does not minimize the FAR. FIR is the probability that an authorized person is identified but is assigned a false ID.

QUESTION 902

The MOST effective control for addressing the risk of piggybacking is:

- a single entry point with a receptionist.
- the use of smart cards.
- a biometric door lock.
- a deadman door.

Correct Answer: D

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Deadman doors use a pair of doors. For the second door to operate, the first entry door must close and lock with only one person permitted in the holding area. This reduces the risk of an unauthorized person following an authorized person through a secured entry (piggybacking). The other choices are all physical controls over entry to a secure area but do not specifically address the risk of piggybacking.

QUESTION 903
The BEST overall quantitative measure of the performance of biometric control devices is:

- false-rejection rate.
- false-acceptance rate.
- equal-error rate.
- estimated-error rate.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
A low equal-error rate (EER) is a combination of a low false-rejection rate and a low false-acceptance rate. EER, expressed as a percentage, is a measure of the number of times that the false-rejection and false-acceptance rates are equal. A low EER is the measure of the more effective biometrics control device. Low false-rejection rates or low false-acceptance rates alone do not measure the efficiency of the device. Estimated-error rate is nonexistent and therefore irrelevant.

QUESTION 904
Which of the following is the MOST effective control over visitor access to a data center?

- Visitors are escorted.
- Visitor badges are required.
- Visitors sign in.
- Visitors are spot-checked by operators.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Escorting visitors will provide the best assurance that visitors have permission to access the data processing facility. Choices B and C are not reliable controls. Choice D is incorrect because visitors should be accompanied at all times while they are on the premises, not only when they are in the data processing facility.

QUESTION 905
The use of residual biometric information to gain unauthorized access is an example of which of the following attacks?

- Replay
- Brute force
- Cryptographic
- Mimic

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Residual biometric characteristics, such as fingerprints left on a biometric capture device, may be reused by an attacker to gain unauthorized access. A brute force attack involves feeding the biometric capture device numerous different biometric samples. A cryptographic attack targets the algorithm or the encrypted data; in a mimic attack, the attacker reproduces characteristics similar to those of the enrolled user, such as forging a signature or imitating a voice.

QUESTION 906
A firm is considering using biometric fingerprint identification on all PCs that access critical data. This requires:

- that a registration process is executed for all accredited PC users.
- the full elimination of the risk of a false acceptance.
- the usage of the fingerprint reader be accessed by a separate password.
- assurance that it will be impossible to gain unauthorized access to critical data.

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The fingerprints of accredited users need to be read, identified, and recorded, i.e., registered, before a user may operate the system from the screened PCs. Choice B is incorrect, as the false-acceptance risk of a biometric device may be optimized, but will never be zero because this would imply an unacceptably high risk of false rejection. Choice C is incorrect, as the fingerprint device reads the token (the user's fingerprint) and does not need to be protected in itself by a password. Choice D is incorrect because the usage of biometric protection on PCs does not guarantee that other potential security weaknesses in the system may not be exploited to access protected data.

QUESTION 907
Which of the following biometrics has the highest reliability and lowest false-acceptance rate (FAR)?

- Palm scan
- Face recognition
- Retina scan
- Hand geometry

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Retina scan uses optical technology to map the capillary pattern of an eye's retina. This is highly reliable and has the lowest false-acceptance rate (FAR) among the current biometric methods. Use of palm scanning entails placing a hand on a scanner where a palm's physical characteristics are captured. Hand geometry, one of the oldest techniques, measures the physical characteristics of the user's hands and fingers from a three-dimensional perspective. The palm and hand biometric techniques lack uniqueness in the geometry data. In face biometrics, a reader analyzes the images captured for general facial characteristics. Though considered a natural and friendly biometric, the main disadvantage of face recognition is the lack of uniqueness, which means that people looking alike can fool the device.

QUESTION 908
The MOST likely explanation for a successful social engineering attack is:

- that computers make logic errors.
- that people make judgment errors.
- the computer knowledge of the attackers.
- the technological sophistication of the attack method.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Humans make errors in judging others; they may trust someone when, in fact, the person is untrustworthy. Driven by logic, computers make the same error every time they execute the erroneous logic; however, this is not the basic argument in designing a social engineering attack. Generally, social engineering attacks do not require technological expertise; often, the attacker is not proficient in information technology or systems. Social engineering attacks are human-based and generally do not involve complicated technology.

QUESTION 909
The purpose of a deadman door controlling access to a computer facility is primarily to:

- prevent piggybacking.
- prevent toxic gases from entering the data center.
- starve a fire of oxygen.
- prevent an excessively rapid entry to, or exit from, the facility.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The purpose of a deadman door controlling access to a computer facility is primarily intended to prevent

piggybacking. Choices B and C could be accomplished with a single self-closing door. Choice D is invalid, as a rapid exit may be necessary in some circumstances, e.g., a fire.

QUESTION 910

Which of the following is the MOST reliable form of single-factor personal identification?

- Smart card
- Password
- Photo identification
- Iris scan

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Since no two irises are alike, identification and verification can be done with confidence. There is no guarantee that a smart card is being used by the correct person since it can be shared, stolen, or lost and found. Passwords can be shared and, if written down, carry the risk of discovery. Photo IDs can be forged or falsified.

QUESTION 911

A data center has a badge-entry system. Which of the following is MOST important to protect the computing assets in the center?

- Badge readers are installed in locations where tampering would be noticed.
- The computer that controls the badge system is backed up frequently.
- A process for promptly deactivating lost or stolen badges exists.
- All badge entry attempts are logged.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Tampering with a badge reader cannot open the door, so this is irrelevant. Logging the entry attempts may be of limited value. The biggest risk is from unauthorized individuals who can enter the data center, whether they are employees or not. Thus, a process of deactivating lost or stolen badges is important. The configuration of the system does not change frequently; therefore, frequent backup is not necessary.

QUESTION 912

Which of the following physical access controls effectively reduces the risk of piggybacking?

- Biometric door locks
- Combination door locks
- Deadman doors
- Bolting door locks

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Deadman doors use a pair of doors. For the second door to operate, the first entry door must close and lock with only one person permitted in the holding area. This effectively reduces the risk of piggybacking. An individual's unique body features such as voice, retina, fingerprint, or signature activate biometric door locks; however, they do not prevent or reduce the risk of piggybacking. Combination door locks, also known as cipher locks, use a numeric keypad or dial

QUESTION 913

The MOST effective biometric control system is the one:

- which has the highest equal-error rate (EER).
- which has the lowest EER.

- for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
- for which the FRR is equal to the failure-to-enroll rate (FER).

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The equal-error rate (EER) of a biometric system denotes the percent at which the false-acceptance rate (FAR) is equal to the false-rejection rate (FRR). The biometric that has the lowest EER is the most effective. The biometric that has the highest EER is the most ineffective. For any biometric, there will be a measure at which the FRR will be equal to the FAR. This is the EER. FER is an aggregate measure of FRR.

QUESTION 914
Which of the following is the BEST way to satisfy a two-factor user authentication?

- A smart card requiring the user's PIN
- User ID along with password
- Iris scanning plus fingerprint scanning
- A magnetic card requiring the user's PIN

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
A smart card addresses what the user has. This is generally used in conjunction with testing what the user knows, e.g., a keyboard password or personal identification number (PIN). An ID and password, what the user knows, is a single-factor user authentication. Choice C is not a two-factor user authentication because it is only biometric. Choice D is similar to choice A, but the magnetic card may be copied; therefore, choice A is the best way to satisfy a two-factor user authentication.

QUESTION 915
What should an organization do before providing an external agency physical access to its information processing facilities (IPFs)?

- The processes of the external agency should be subjected to an IS audit by an independent agency.
- Employees of the external agency should be trained on the security procedures of the organization.
- Any access by an external agency should be limited to the demilitarized zone (DMZ).
- The organization should conduct a risk assessment and design and implement appropriate controls.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Physical access of information processing facilities (IPFs) by an external agency introduces additional threats into an organization. Therefore, a risk assessment should be conducted and controls designed accordingly. The processes of the external agency are not of concern here. It is the agency's interaction with the organization that needs to be protected. Auditing their processes would not be relevant in this scenario. Training the employees of the external agency may be one control procedure but could be performed after access has been granted. Sometimes an external agency may require access to the processing facilities beyond the demilitarized zone (DMZ). For example, an agency that undertakes maintenance of servers may require access to the main server room. Restricting access within the DMZ will not serve the purpose.

QUESTION 916
An IS auditor is reviewing the physical security measures of an organization. Regarding the access card system, the IS auditor should be MOST concerned that:

- nonpersonalized access cards are given to the cleaning staff, who use a sign-in sheet but show no proof of identity.
- access cards are not labeled with the organization's name and address to facilitate easy return of a lost card.

- card issuance and rights administration for the cards are done by different departments, causing unnecessary lead time for new cards.
- the computer system used for programming the cards can only be replaced after three weeks in the event of a system failure.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Physical security is meant to control who is entering a secured area, so identification of all individuals is of utmost importance. It is not adequate to trust unknown external people by allowing them to write down their alleged name without proof, e.g., identity card, driver's license. Choice B is not a concern because if the name and address of the organization were written on the card, a malicious finder could use the card to enter the organization's premises. Separating card issuance from technical rights management is a method to ensure a proper segregation of duties so that no single person can produce a functioning card for a restricted area within the organization's premises. Choices B and C are good practices, not concerns. Choice D may be a concern, but not as important since a system failure of the card programming device would normally not mean that the readers do not function anymore. It simply means that no new cards can be issued, so this option is minor compared to the threat of improper identification.

QUESTION 917
Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

- Overwriting the tapes
- Initializing the tape labels
- Degaussing the tapes
- Erasing the tapes

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The best way to handle obsolete magnetic tapes is to degauss them. This action leaves a very low residue of magnetic induction, essentially erasing the data from the tapes. Overwriting or erasing the tapes may cause magnetic errors but would not remove the data completely. Initializing the tape labels would not remove the data that follows the label.

QUESTION 918
Which of the following is the MOST important objective of data protection?

- identifying persons who need access to information
- Ensuring the integrity of information
- Denying or authorizing access to the IS system
- Monitoring logical accesses

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Maintaining data integrity is the most important objective of data security. This is a necessity if an organization is to continue as a viable and successful enterprise. The other choices are important techniques for achieving the objective of data integrity.

QUESTION 919
Which of the following aspects of symmetric key encryption influenced the development of asymmetric encryption?

- Processing power
- Volume of data
- Key distribution
- Complexity of the algorithm

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Symmetric key encryption requires that the keys be distributed. The larger the user group, the more challenging the key distribution. Symmetric key cryptosystems are generally less complicated and, therefore, use less processing power than asymmetric techniques, thus making it ideal for encrypting a large volume of data. The major disadvantage is the need to get the keys into the hands of those with whom you want to exchange data, particularly in e-commerce environments, where customers are unknown, untrusted entities.

QUESTION 920
A hard disk containing confidential data was damaged beyond repair. What should be done to the hard disk to prevent access to the data residing on it?

- Rewrite the hard disk with random Os and Is.
- Low-level format the hard disk.
- Demagnetize the hard disk.
- Physically destroy the hard disk.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Physically destroying the hard disk is the most economical and practical way to ensure that the data cannot be recovered. Rewriting data and low-level formatting are impractical because the hard disk is damaged. Demagnetizing is an inefficient procedure, as it requires specialized and expensive equipment to be fully effective.

QUESTION 921
Which of the following is the MOST robust method for disposing of magnetic media that contains confidential information?

- Degaussing
- Defragmenting
- Erasing
- Destroying

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Destroying magnetic media is the only way to assure that confidential information cannot be recovered. Degaussing or demagnetizing is not sufficient to fully erase information from magnetic media. The purpose of defragmentation is to eliminate fragmentation in file systems and does not remove information. Erasing or deleting magnetic media does not remove the information; this method simply changes a file's indexing information.

QUESTION 922
Which of the following would MOST effectively control the usage of universal storage bus (USB) storage devices?

- Policies that require instant dismissal if such devices are found
- Software for tracking and managing USB storage devices
- Administratively disabling the USB port
- Searching personnel for USB storage devices at the facility's entrance

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Software for centralized tracking and monitoring would allow a USB usage policy to be applied to each user based on changing business requirements, and would provide for monitoring and reporting exceptions to management. A policy requiring dismissal may result in increased employee attrition, and business requirements would not be

properly addressed. Disabling ports would be complex to manage and might not allow for new business needs. Searching personnel for USB storage devices at the entrance to a facility is not a practical solution since these devices are small and could be easily hidden.

QUESTION 923

An organization is disposing of a number of laptop computers. Which of the following data destruction methods would be the MOST effective?

- Run a low-level data wipe utility on all hard drives
- Erase all data file directories
- Format all hard drives
- Physical destruction of the hard drive

Correct Answer: D

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

The most effective method is physical destruction. Running a low-level data wipe utility may leave some residual data that could be recovered; erasing data directories and formatting hard drives are easily reversible, exposing all data on the drive to unauthorized individuals.

QUESTION 924

To ensure authentication, confidentiality, and integrity of a message, the sender should:

- Encrypt the hash of the message with the sender's public key and then encrypt the message with the receiver's private key.
- Encrypt the hash of the message with the sender's private key and then encrypt the message with the receiver's public key.
- Encrypt the hash of the message with the sender's public key and then encrypt the message with the receiver's public key.
- Encrypt the hash of the message with the sender's private key and then encrypt the message with the receiver's private key.

Correct Answer: B

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Obtaining the hash of the message ensures integrity; signing the hash of the message with the sender's private key ensures the authenticity of the origin, and encrypting the resulting message with the receiver's public key ensures confidentiality. The other choices are incorrect.

QUESTION 925

Which of the following would be the MOST significant audit finding when reviewing a point-of-sale (POS) system?

- Invoices recorded on the POS system are manually entered into an accounting application
- An optical scanner is not used to read bar codes for the generation of sales invoices
- Frequent power outages occur, resulting in the manual preparation of invoices
- Customer credit card information is stored unencrypted on the local POS system

Correct Answer: D

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

It is important for the IS auditor to determine if any credit card information is stored on the local point-of-sale (POS) system. Any such information, if stored, should be encrypted or protected by other means to avoid the possibility of unauthorized disclosure. Manually inputting sale invoices into the accounting application is an operational issue. The nonavailability of optical scanners to read bar codes of the products and power outages are also operational issues but do not pose the same level of risk as unencrypted credit card information.

QUESTION 926

When reviewing the procedures for the disposal of computers, which of the following should be the GREATEST concern for the IS auditor?

- Hard disks are overwritten several times at the sector level, but are not reformatted before leaving the organization.
- All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving the organization.
- Hard disks are rendered unreadable by hole-punching through the platters at specific positions before leaving the organization.
- The transport of hard disks is escorted by internal security staff to a nearby metal recycling company, where the hard disks are registered and then shredded.

Correct Answer: B

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Deleting and formatting does not completely erase the data but only marks the sectors that contained files as being free. There are tools available over the Internet that allow one to reconstruct most of a hard disk's contents. Overwriting a hard disk at the sector level would completely erase data, directories, indices, and master file tables. While hole-punching does not delete file contents, the hard disk cannot be used anymore, especially when head parking zones and track zero information are impacted.

QUESTION 927

At a hospital, medical personnel carry handheld computers that contain patient health data. These handheld computers are synchronized with PCs that transfer data from a hospital database. Which of the following would be of the most importance?

- The handheld computers are properly protected to prevent loss of data confidentiality, in case of theft or loss.
- The employee who deletes temporary files from the local PC, after usage, is authorized to maintain PCs.
- Timely synchronization is ensured by policies and procedures.
- The usage of the handheld computers is allowed by the hospital policy.

Correct Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Data confidentiality is a major requirement of privacy regulations. Choices B, C, and D relate to internal security requirements, which are secondary compared to compliance with data privacy laws.

QUESTION 928

Which of the following would BEST support 24/7 availability?

- Daily backup
- Offsite storage
- Mirroring
- Periodic testing

Correct Answer: C

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Mirroring of critical elements is a tool that facilitates immediate recoverability. Daily backup implies that it is reasonable for restoration to take place within a number of hours but not immediately. Offsite storage and periodic testing of systems do not by themselves support continuous availability.

QUESTION 929

The PRIMARY purpose of implementing Redundant Array of Inexpensive Disks (RAID) level 1 in a file server is to:

- Achieve performance improvement.
- Provide user authentication.

- Ensure availability of data.
- Ensure the confidentiality of data.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
RAID level 1 provides disk mirroring. Data written to one disk are also written to another disk. Users in the network access data in the first disk; if disk one fails, the second disk takes over. This redundancy ensures the availability of data. RAID level 1 does not improve performance, has no relevance to authentication, and does nothing to provide for data confidentiality.

QUESTION 930
Which of the following is the MOST important criterion when selecting a location for an offsite storage facility for IS backup files? The offsite facility must be:

- Physically separated from the data center and not subject to the same risks.
- Given the same level of protection as that of the computer data center.
- Outsourced to a reliable third party.
- Equipped with surveillance capabilities.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
It is important that there be an offsite storage location for IS files and that it be in a location not subject to the same risks as the primary data center. The other choices are all issues that must be considered when establishing the offsite location, but they are not as critical as the location selection.

QUESTION 931
If a database is restored using before-image dumps, where should the process begin following an interruption?

- Before the last transaction
- After the last transaction
- As the first transaction after the latest checkpoint
- As the last transaction before the latest checkpoint

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
If before images are used, the last transaction in the dump will not have updated the database prior to the dump being taken. The last transaction will not have updated the database and must be reprocessed. Program checkpoints are irrelevant in this situation.

QUESTION 932
In addition to the backup considerations for all systems, which of the following is an important consideration in providing backup for online systems?

- Maintaining system software parameters
- Ensuring periodic dumps of transaction logs
- Ensuring grandfather-father-son file backups
- Maintaining important data at an offsite location

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Ensuring periodic dumps of transaction logs is the only safe way of preserving timely historical data. The volume of activity usually associated with an online system makes other more traditional methods of backup impractical.

QUESTION 933

As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up on tape. During the backup procedure, a drive malfunctions and the order entry files are lost. Which of the following is necessary to restore these files?

- The previous day's backup file and the current transaction tape
- The previous day's transaction file and the current transaction tape
- The current transaction tape and the current hard copy transaction log
- The current hard copy transaction log and the previous day's transaction file

Correct Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

The previous day's backup file will be the most current historical backup of activity in the system. The current day's transaction file will contain all of the day's activity. Therefore, the combination of these two files will enable full recovery up to the point of interruption.

QUESTION 934

An offsite information processing facility:

- Should have the same amount of physical access restrictions as the primary processing site.
- Should be easily identified from the outside so that, in the event of an emergency, it can be easily found.
- Should be located in proximity to the originating site, so it can quickly be made operational.
- Need not have the same level of environmental monitoring as the originating site.

Correct Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

An offsite information processing facility should have the same amount of physical control as the originating site. It should not be easily identified from the outside to prevent intentional sabotage. The offsite facility should not be subject to the same natural disaster that could affect the originating site and thus should not be located in proximity to the original site. The offsite facility should possess the same level of environmental monitoring and control as the originating site.

QUESTION 935

An IS auditor performing a review of the backup processing facilities should be MOST concerned that:

- Adequate fire insurance exists.
- Regular hardware maintenance is performed.
- Offsite storage of transaction and master files exists.
- Backup processing facilities are fully tested.

Correct Answer: C

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

QUESTION 936

Which of the following procedures would BEST determine whether adequate recovery/restart procedures exist?

- Reviewing program code
- Reviewing operations documentation
- Turning off the UPS, then the power
- Reviewing program documentation

Correct Answer: B

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Operations documentation should contain recovery/restart procedures, so operations can return to normal processing in a timely manner. Turning off the uninterruptible power supply (UPS) and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The review of program code and documentation generally does not provide evidence regarding recovery/restart procedures.

QUESTION 937
Which of the following findings should an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?

- There are three individuals with a key to enter the area.
- Paper documents are also stored in the offsite vault.
- Data files that are stored in the vault are synchronized.
- The offsite vault is located in a separate facility.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not correct because an IS auditor would not be concerned with whether paper documents are stored in the offsite vault. In fact, paper documents, such as procedural documents and a copy of the contingency plan, would most likely be stored in the offsite vault, and the location of the vault is important, but not as important as the files being synchronized.

QUESTION 938
Online banking transactions are being posted to the database when processing suddenly comes to a halt. The integrity of the transaction processing is BEST ensured by:

- Database integrity checks.
- Validation checks.
- Input controls.
- Database commits and rollbacks.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Database commits ensure the data are saved to disk, while the transaction processing is underway or complete. Rollback ensures that the already completed processing is reversed back, and the data already processed are not saved to the disk in the event of the failure of the completion of the transaction processing. All other options do not ensure integrity while processing is underway.

QUESTION 939
To provide protection for media backup stored at an offsite location, the storage site should be:

- Located on a different floor of the building.
- Easily accessible by everyone.
- Clearly labeled for emergency access.
- Protected from unauthorized access.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The offsite storage site should always be protected against unauthorized access and have at least the same security requirements as the primary site. Choice A is incorrect because if the backup is in the same building, it may suffer the same event and may be inaccessible. Choices B and C represent access risks.

QUESTION 940

Which of the following ensures the availability of transactions in the event of a disaster?

- Send tapes hourly containing transactions offsite.
- Send tapes daily containing transactions offsite.
- Capture transactions to multiple storage devices.
- Transmit transactions offsite in real time.

Correct Answer: D

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

The only way to ensure availability of all transactions is to perform a real-time transmission to an offsite facility. Choices A and B are not in real time and, therefore, would not include all the transactions. Choice C does not ensure availability at an offsite location.

QUESTION 941

IS management has decided to install a level 1 Redundant Array of Inexpensive Disks (RAID) system in all servers to compensate for the elimination of offsite backups. The IS auditor should recommend:

- Upgrading to a level 5 RAID.
- Increasing the frequency of onsite backups.
- Reinstating the offsite backups.
- Establishing a cold site in a secure location.

Correct Answer: C

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

A RAID system, at any level, will not protect against a natural disaster. The problem will not be alleviated without offsite backups, more frequent onsite backups, or even setting up a cold site. Choices A, B, and D do not compensate for the lack of offsite backup.

QUESTION 942

In which of the following situations is it MOST appropriate to implement data mirroring as the recovery strategy?

- Disaster tolerance is high.
- Recovery time objective is high.
- Recovery point objective is low.
- Recovery point objective is high.

Correct Answer: C

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

A recovery point objective (RPO) indicates the latest point in time at which it is acceptable to recover the data. If the RPO is low, data mirroring should be implemented as the data recovery strategy. The recovery time objective (RTO) is an indicator of disaster tolerance. The lower the RTO, the lower the disaster tolerance.

QUESTION 943

Network Data Management Protocol (NDMP) technology should be used for backup if:

- A network attached storage (NAS) appliance is required.
- The use of TCP/IP must be avoided.
- File permissions that cannot be handled by legacy backup systems must be backed up.
- Backup consistency over several related data volumes must be ensured.

Correct Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

NDMP is particularly useful for NAS environments where it is challenging to install backup software agents. NDMP optimizes backup performance and addresses the challenges of backing up NAS devices.

QUESTION 944

An organization currently using tape backups takes one full backup weekly and incremental backups daily. They recently augmented their tape backup procedures with a backup-to-disk solution. This is appropriate because:

- Fast synthetic backups for offsite storage are supported.
- Backup to disk is always significantly faster than backup to tape.
- Tape libraries are no longer needed.
- Data storage on disks is more reliable than on tapes.

Correct Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Disk-to-disk (D2D) backup is not a direct replacement for tape but enhances the backup architecture. It enables fast synthetic backups, which can improve recovery performance.

QUESTION 945

Which of the following should be the MOST important criterion in evaluating a backup solution for sensitive data that must be retained for a long period due to regulatory requirements?

- Full backup window
- Media costs
- Restore window
- Media reliability

Correct Answer: D

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Media reliability is crucial for ensuring the organization's ability to recover data, especially for compliance with regulatory requirements. Other factors, while important, should not take precedence over media reliability.

QUESTION 946

In the event of a data center disaster, which of the following would be the MOST appropriate strategy to enable a complete recovery of a critical database?

- Daily data backup to tape and storage at a remote site
- Real-time replication to a remote site
- Hard disk mirroring to a local server
- Real-time data backup to the local storage area network (SAN)

Correct Answer: B

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Real-time replication to a remote site ensures that data is continuously updated, minimizing data loss during a disaster. Other options may not provide the same level of protection against data loss.

QUESTION 947

Which of the following backup techniques is the MOST appropriate when an organization requires extremely granular data restore points, as defined in the recovery point objective (RPO)?

- Virtual tape libraries
- Disk-based snapshots
- Continuous data backup
- Disk-to-tape backup

Correct Answer: C

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Continuous data backup allows for real-time data protection, ensuring extremely granular restore points that align with a low RPO.

QUESTION 948
What is the BEST backup strategy for a large database with data supporting online sales?

- Weekly full backup with daily incremental backup
- Daily full backup
- Clustered servers
- Mirrored hard disks

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A weekly full backup combined with daily incremental backups balances recovery capabilities and minimizes daily backup times, making it practical for a large database.

QUESTION 949
During an audit, an IS auditor notes that an organization's business continuity plan (BCP) does not adequately address information confidentiality during a recovery process. The IS auditor should recommend that the plan be modified to include:

- The level of information security required when business recovery procedures are invoked.
- Information security roles and responsibilities in the crisis management structure.
- Information security resource requirements.
- Change management procedures for information security that could affect business continuity arrangements.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
It's essential for the BCP to specify the level of information security needed during recovery, especially regarding access to confidential data.

QUESTION 950
Which of the following is the GREATEST risk when storage growth in a critical file server is not managed properly?

- Backup time would steadily increase
- Backup operational cost would significantly increase
- Storage operational cost would significantly increase
- Server recovery work may not meet the recovery time objective (RTO)

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
If the growth of data is unmanaged, the time required to recover the server may exceed the RTO, leading to significant operational issues.