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.
