**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.