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

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

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

QUESTION 202
If a database is restored from information backed up before the last system image, which of the following is recommended?

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

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

QUESTION 203
An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

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

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

QUESTION 204
Which of the following is the dominating objective of BCP and DRP?

- **A)** To protect human life
- **B)** To mitigate the risk and impact of a business interruption
- **C)** To eliminate the risk and impact of a business interruption
- **D)** To transfer the risk and impact of a business interruption

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

QUESTION 205
How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

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

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

QUESTION 206

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

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

Correct Answer: A

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

QUESTION 207

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

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

Correct Answer: D

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

QUESTION 208

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

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

Correct Answer: C

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

QUESTION 209

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

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

Correct Answer: D

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

QUESTION 210

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

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

Correct Answer: D

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

QUESTION 211
What uses questionnaires to lead the user through a series of choices to reach a conclusion?
- **A)** Logic trees
- **B)** Decision trees
- **C)** Decision algorithms
- **D)** Logic algorithms

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

QUESTION 212
What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?
- **A)** Assigning copyright to the organization
- **B)** Program back doors
- **C)** Source code escrow
- **D)** Internal programming expertise

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

QUESTION 213
Who is ultimately responsible for providing requirement specifications to the software-development team?
- **A)** The project sponsor
- **B)** The project members
- **C)** The project leader
- **D)** The project steering committee

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

QUESTION 214
What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?
- **A)** Contrived data
- **B)** Independently created data
- **C)** Live data
- **D)** Data from previous tests

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

QUESTION 215
An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to:
- **A)** Meet business objectives
- **B)** Enforce data security
- **C)** Be culturally feasible
- **D)** Be financially feasible

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

QUESTION 216
Which of the following processes are performed during the design phase of the systems-development life cycle (SDLC) model?

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

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

QUESTION 217
When should application controls be considered within the system-development process?

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

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

QUESTION 218
What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality?

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

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

QUESTION 219
Test and development environments should be separated. True or false?

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

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

QUESTION 220
What kind of testing should programmers perform following any changes to an application or system?

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

Correct Answer: A
Explanation: Following any changes to an application or system, programmers should perform unit,

module, and full regression testing to ensure the changes work as intended and do not introduce new issues.

QUESTION 221
Which of the following uses a prototype that can be updated continually to meet changing user or business requirements?

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

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

QUESTION 222
What is the most common reason for information systems to fail to meet the needs of users? Choose the BEST answer.

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

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

QUESTION 223
Who is responsible for the overall direction, costs, and timetables for systems-development projects?

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

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

QUESTION 224
When should plans for testing for user acceptance be prepared? Choose the BEST answer.

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

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

QUESTION 225
Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

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

- **Insufficient unit, module, and systems testing**

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

QUESTION 226
Input/output controls should be implemented for which applications in an integrated systems environment?

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

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

QUESTION 227
Authentication techniques for sending and receiving data between EDI systems are crucial to prevent which of the following? Choose the BEST answer.

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

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

QUESTION 228
After identifying potential security vulnerabilities, what should be the IS auditor's next step?

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

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

QUESTION 229
What is the primary security concern for EDI environments? Choose the BEST answer.

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

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

QUESTION 230
Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?

- **Exposures**
- **Threats** (Correct)

- **Hazards**
- **Insufficient controls**

Explanation:
Threats exploit vulnerabilities, leading to potential loss or damage to the organization's assets.

QUESTION 231
Business process re-engineering often results in _____ automation, which results in _____ number of people using technology. Fill in the blanks.

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

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

QUESTION 232
Whenever business processes have been re-engineered, the IS auditor attempts to identify and quantify the impact of any controls that might have been removed or controls that might not work as effectively after business process changes. True or false?

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

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

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

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

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

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

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

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

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

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

- **Accuracy check**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

QUESTION 241
An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

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

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

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

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

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

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

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

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

QUESTION 244
Which of the following is a substantive test?

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

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

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

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

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

QUESTION 246
An audit charter should:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

QUESTION 252
The PRIMARY purpose of audit trails is to:

- improve response time for users.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

QUESTION 257
In planning an audit, the MOST critical step is the identification of the:
- **areas of high risk.** (Correct)
- skill sets of the audit staff.
- test steps in the audit.
- time allotted for the audit.

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

QUESTION 258
The extent to which data will be collected during an IS audit should be determined based on the:
- availability of critical and required information.
- auditor's familiarity with the circumstances.
- auditee's ability to find relevant evidence.
- **purpose and scope of the audit being done.** (Correct)

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

QUESTION 259
While planning an audit, an assessment of risk should be made to provide:
- **reasonable assurance that the audit will cover material items.** (Correct)
- definite assurance that material items will be covered during the audit work.
- reasonable assurance that all items will be covered by the audit.
- sufficient assurance that all items will be covered during the audit work.

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

QUESTION 260
An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling when:
- **the probability of error must be objectively quantified.** (Correct)
- the auditor wishes to avoid sampling risk.
- generalized audit software is unavailable.
- the tolerable error rate cannot be determined.

Section: IS AUDIT PROCESS
Explanation:
Statistical sampling allows for the objective quantification of error probabilities, which is necessary when the auditor needs to provide numerical confidence levels. Judgmental sampling, on the other hand, relies

on the auditor's experience but does not offer the same objective measurement. Sampling risk exists in both methods.

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

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

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

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

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

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

QUESTION 263
An IS auditor evaluating logical access controls should FIRST:

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

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

QUESTION 264
The PRIMARY purpose of an IT forensic audit is:

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

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

QUESTION 265

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

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

  Correct Answer: D

  Explanation:

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

QUESTION 266

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

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

  Correct Answer: D

  Explanation:

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

QUESTION 267

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

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

  Correct Answer: D

  Explanation:

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

QUESTION 268

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

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

  Correct Answer: A

  Explanation:

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

QUESTION 269

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

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

Correct Answer: A

Explanation:

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

QUESTION 270

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

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

Correct Answer: B

Explanation:

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

QUESTION 271

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

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

Correct Answer: D

Explanation:

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

QUESTION 272

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

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

Correct Answer: D

Explanation:

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

QUESTION 273

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

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

  Correct Answer: A

  Explanation:

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

QUESTION 274

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

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

  Correct Answer: A

  Explanation:

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

QUESTION 275

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

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

  Correct Answer: A

  Explanation:

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

QUESTION 276

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

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

  Correct Answer: C

  Explanation:

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

QUESTION 277

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

- A. Test data to validate data input
- B. Test data to determine system sort capabilities

- C. Generalized audit software to search for address field duplications
- D. Generalized audit software to search for account field duplications

Correct Answer: C

Explanation:

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

QUESTION 278

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

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

Correct Answer: A

Explanation:

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

QUESTION 279

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

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

Correct Answer: D

Explanation:

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

QUESTION 280

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

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

Correct Answer: A

Explanation:

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

QUESTION 281

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

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

Correct Answer: D

Explanation:

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

QUESTION 282

An IS auditor reviews an organizational chart PRIMARILY for:

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

Correct Answer: C

Explanation:

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

QUESTION 283

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

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

Correct Answer: A

Explanation:

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

QUESTION 284

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

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

Correct Answer: B

Explanation:

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

QUESTION 285

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

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

Correct Answer: B

Explanation:

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

QUESTION 286

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

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

Correct Answer: C

Explanation:

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

QUESTION 287

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

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

Correct Answer: C

Explanation:

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

QUESTION 288

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

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

Correct Answer: B

Explanation:

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

QUESTION 289

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

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

Correct Answer: A

Explanation:

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

QUESTION 290

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

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

Correct Answer: D

Explanation:

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

QUESTION 291

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

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

Correct Answer: A

Explanation:

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

QUESTION 292

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

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

Correct Answer: C

Explanation:

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

QUESTION 293

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

- A. determining whether bar code readers are installed.

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

Correct Answer: C

Explanation:

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

QUESTION 294

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

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

Correct Answer: C

Explanation:

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

QUESTION 295

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

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

Correct Answer: B

Explanation:

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

QUESTION 296

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

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

Correct Answer: A

Explanation:

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

QUESTION 297

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

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

Correct Answer: A

Explanation:

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

QUESTION 298

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

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

Correct Answer: A

Explanation:

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

QUESTION 299

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

- A. confirm that the auditors did not overlook any important issues.
- B. gain agreement on the findings.
- C. receive feedback on the adequacy of the audit procedures.
- D. test the structure of the final presentation.

Correct Answer: B

Explanation:

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

QUESTION 300

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

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

Correct Answer: C

Explanation:

An automated code comparison is the most efficient and effective technique for detecting unauthorized

program changes. It directly compares the current and previous versions of the program to identify any unauthorized alterations. Test data runs and code reviews are less efficient and do not directly address unauthorized changes.