PassQueen
a.k.a dumpsqueen.com

Certified Information Systems Auditor

Isaca CISA

Version Demo

Total Demo Questions: 70

Total Premium Questions: 706

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Information Systems Auditing Process	121
Topic 2, Governance and Management of IT	93
Topic 3, Information Systems Acquisition, Development and Implementation	116
Topic 4, Information Systems Operations and Business Resilience	110
Topic 5, Protection of Information Assets	266
Total	706

QUESTION NO: 1

The PRIMARY objective of value delivery in reference to IT governance is to:

A. promote best practices

B. increase efficiency.

C. optimize investments.

D. ensure compliance.

ANSWER: C

Explanation:

Optimize investments is correct because value delivery in IT governance is concerned with ensuring that IT-enabled investments produce the intended business benefits at an acceptable cost and with appropriate risk. Governance directs decision makers to select, prioritize, fund, and monitor initiatives according to their contribution to enterprise objectives. This includes realizing planned benefits throughout an investment's life cycle, not merely approving a project or implementing technology. In practical terms, value delivery requires the organization to balance benefits realization, resource use, costs, and risk so that the portfolio of IT services, programs, and assets delivers the greatest sustainable value to stakeholders. ISACA's COBIT framework identifies benefits realization as a central governance objective and emphasizes optimizing value from IT-enabled investments through alignment with enterprise goals, portfolio oversight, and performance monitoring. This focus makes investment optimization the primary objective of value delivery. Further information is available from ISACA's COBIT resources and ISACA's overview of the COBIT framework.

QUESTION NO: 2

During a project audit, an IS auditor notes that project reporting does not accurately reflect current progress. Which of the following is the GREATEST resulting impact?

A. The project manager will have to be replaced.

B. The project reporting to the board of directors will be incomplete.

C. The project steering committee cannot provide effective governance.

D. The project will not withstand a quality assurance (QA) review.

ANSWER: C

Explanation:

The project steering committee cannot provide effective governance. Accurate, timely project-status reporting is a fundamental input to governance because it enables the steering committee to oversee delivery, evaluate whether the project remains aligned with its business case and objectives, identify material risks and issues, and make informed decisions on priorities, resources, scope, funding, or corrective action. If reported progress differs from actual progress, the committee may make decisions based on an unreliable view of schedule, cost, deliverables, dependencies, and risk exposure. This impairs its ability to exercise appropriate oversight and accountability at the point where intervention can be most valuable. Project governance is not limited to receiving reports; it relies on dependable information to direct and monitor the project throughout its life cycle. ISACA describes governance as ensuring stakeholder needs are evaluated and that direction and monitoring are performed, activities that require reliable performance information. Guidance from the Project Management Institute likewise emphasizes monitoring and controlling project work through the collection and assessment of performance data. See ISACA COBIT resources and PMI guidance on monitoring and controlling project work.

QUESTION NO: 3

Which of the following should an IS auditor review FIRST when planning a customer data privacy audit?

A. Legal and compliance requirements

B. Customer agreements

C. Data classification

D. Organizational policies and procedures

ANSWER: A

Explanation:

Legal and compliance requirements should be reviewed first because they establish the authoritative privacy obligations against which the audit scope, objectives, criteria, and risk assessment must be designed. Customer-data processing may be governed by privacy statutes, sector-specific rules, regulator guidance, cross-border transfer requirements, breach-notification duties, and retention or data-subject-rights obligations. Identifying which requirements apply to the organization, its customers, its jurisdictions, and the relevant processing activities enables the auditor to define meaningful control expectations and determine the evidence needed during the audit. This initial regulatory baseline also supports a risk-based plan by highlighting obligations with significant potential legal, financial, and reputational impact. The resulting audit criteria can then be used to assess whether internal governance, data-handling practices, and contractual commitments implement the required protections. The NIST Privacy Framework similarly emphasizes identifying privacy requirements and managing privacy risk as a foundation for organizational privacy governance. ISACA's privacy guidance also positions compliance and governance as central elements of an effective privacy program. See the NIST Privacy Framework and ISACA Privacy resources.

QUESTION NO: 4

Which of the following is the BEST indicator for measuring performance of IT help desk function?

A. Percentage of problems raised from incidents

B. Mean time to categorize tickets

C. Number of incidents reported

D. Number of reopened tickets

ANSWER: D

Explanation:

Number of reopened tickets is the best indicator because it directly reflects whether the help desk resolved users' issues effectively and durably at the point a ticket was initially closed. A reopened ticket means that the reported issue either persisted, recurred, or was not resolved to the user's satisfaction. Tracking this measure therefore provides meaningful evidence about the quality and effectiveness of ticket handling, including diagnosis, communication with users, resolution validation, and closure practices.

This metric is especially useful to management and auditors because it highlights potential gaps in the end-to-end support process rather than merely recording the volume or speed of activity. Trends in reopened tickets can identify recurring technical issues, insufficient knowledge articles, premature closure practices, or a need for additional analyst training. The measure can also be segmented by support group, category, priority, or service to target improvement actions. For sound performance measurement, the help desk should define what qualifies as a reopening, establish a reporting period, and review the rate in context with ticket volume and customer feedback. Guidance on service-desk metrics recognizes ticket reopen rate as a useful indicator of resolution quality; see Zendesk's help desk metrics guidance and Atlassian's ITSM metrics guidance.

QUESTION NO: 5

A new regulation in one country of a global organization has recently prohibited cross-border transfer of personal data. An IS auditor has been asked to determine the organization's level of exposure In the affected country. Which of the following would be MOST helpful in making this assessment?

A. Developing an inventory of all business entities that exchange personal data with the affected jurisdiction

B. Identifying data security threats in the affected jurisdiction

C. Reviewing data classification procedures associated with the affected jurisdiction

D. Identifying business processes associated with personal data exchange with the affected jurisdiction

ANSWER: D

Explanation:

Identifying business processes associated with personal data exchange with the affected jurisdiction is the most helpful starting point because the organization's exposure arises where operational activities depend on, enable, or cause cross-border transfers of personal data. Mapping those processes allows the auditor to determine what personal data is transferred, the sending and receiving locations, the systems and third parties involved, the transfer frequency and volume, and the business services that could be disrupted or become noncompliant. This creates a direct, risk-based view of regulatory exposure and supports prioritization of remediation, such as changing process design, localizing data, or implementing an approved lawful transfer mechanism if one is available. A process-focused assessment also connects the legal restriction to accountable business owners and relevant controls, making the results actionable for management. ISACA's privacy guidance emphasizes understanding data flows and the processing context to manage privacy risk effectively. Similarly, the NIST Privacy Framework identifies data processing and data-flow understanding as essential to identifying and managing privacy risk. See ISACA's privacy-by-design guidance and the NIST Privacy Framework.

QUESTION NO: 6

Which of the following is the PRIMARY purpose of establishing a recovery point objective (RPO) for a critical business process?

A. To define the maximum acceptable amount of data loss.

B. To establish the maximum duration of a service outage.

C. To determine the priority sequence for restoring applications.

D. To identify the minimum staffing required at an alternate site.

ANSWER: A

Explanation:

To define the maximum acceptable amount of data loss. is correct because the RPO identifies the point in time to which information must be restored following a disruption. It is expressed as the maximum tolerable period of data that may be lost, such as transactions entered since the most recent successful backup, replication point, or journal capture. The RPO drives requirements for backup frequency, replication design, retention, and recovery procedures. It differs from a recovery time objective, which defines the maximum allowable time to restore a service. NIST contingency-planning guidance describes recovery objectives as being based on business impact and recovery requirements. See NIST SP 800-34 Rev. 1.

QUESTION NO: 7

An IS auditor finds that one employee has unauthorized access to confidential data. The IS auditor's BEST recommendation should be to:

A. reclassify the data to a lower level of confidentiality

B. require the business owner to conduct regular access reviews.

C. implement a strong password schema for users.

D. recommend corrective actions to be taken by the security administrator.

ANSWER: B

Explanation:

Requiring the business owner to conduct regular access reviews is the best recommendation because the business owner is accountable for determining who has a legitimate business need to access confidential information. Periodic access recertification validates that each user's access remains appropriate as job responsibilities, assignments, and employment status change. It also provides a repeatable detective control that can identify excessive, obsolete, or otherwise unauthorized privileges across the population of users, rather than merely addressing the individual instance found by the audit.

Effective access reviews should use defined review intervals based on data sensitivity and risk, identify the owner responsible for approval, require evidence of the review and decisions, and ensure that access identified as no longer needed is removed promptly. This aligns with the principle that system account management includes periodically reviewing accounts for compliance with organizational account-management requirements. For confidential data, owner-led review is particularly important because the owner understands the data's business purpose, classification, and valid access requirements. See NIST SP 800-53 Rev. 5, Account Management (AC-2) and ISACA CISA certification resources.

QUESTION NO: 8

A data center's physical access log system captures each visitor's identification document numbers along with the visitor's photo. Which of the following sampling methods would be MOST useful to an IS auditor conducting compliance testing for the effectiveness of the system?

A. Quota sampling

B. Haphazard sampling

C. Attribute sampling

D. Variable sampling

ANSWER: C

Explanation:

Attribute sampling is correct because the audit objective is compliance testing of a control: determining whether visitor-access-log records consistently contain required attributes, specifically an identification document number and a visitor photo. Each sampled visitor record can be evaluated as a binary outcome—compliant or noncompliant—based on whether the required information is present, accurate, and retained in accordance with the access-control requirement. The auditor can use the sample results to estimate the rate of control deviations in the population and assess whether the physical access log system is operating effectively. This approach aligns with the purpose of attribute sampling in audit work, which is to test the presence or absence of specified characteristics rather than to estimate a numerical quantity. The auditor should define the population, sampling unit, period under review, required attributes, tolerable deviation rate, and expected deviation rate before selecting the sample. Appropriate evidence may include the log entry, associated image, and the approved visitor-access procedure or policy establishing the documentation requirement. ISACA discusses audit sampling considerations at ISACA Journal: Audit Sampling Considerations. Further guidance on designing samples to evaluate control compliance is available in the GAO Financial Audit Manual, Volume 1.

QUESTION NO: 9

When determining whether a project in the design phase will meet organizational objectives, what is BEST to compare against the business case?

A. Implementation plan

B. Project budget provisions

C. Requirements analysis

D. Project plan

ANSWER: C

Explanation:

Requirements analysis is the best comparison because it translates the business case's expected benefits, strategic objectives, scope, and stakeholder needs into specific, testable business and system requirements. During the design phase, an auditor or project reviewer should confirm that the requirements being used to shape the solution remain traceable to the original business justification. This establishes whether the proposed design is capable of delivering the intended organizational value rather than merely meeting technical expectations.

A business case explains why the organization should make the investment, including the desired outcomes and anticipated benefits. Requirements analysis defines what the solution must do, the constraints it must observe, and the acceptance criteria by which successful delivery can be assessed. Comparing these artifacts helps identify gaps, unnecessary requirements, scope drift, or requirements that no longer support the approved objectives. It also supports benefits realization by ensuring that design decisions are grounded in validated business needs throughout the project lifecycle. ISACA emphasizes that governance of enterprise information and technology should align investments and delivery activities with enterprise objectives and value creation. See ISACA's guidance on realizing business benefits from IT investments and the Project Management Institute's discussion of requirements management and validation.

QUESTION NO: 10

In which of the following system development life cycle (SDLC) phases would an IS auditor expect to find that controls have been incorporated into system specifications?

A. Implementation

B. Development

C. Feasibility

D. Design

ANSWER: D

Explanation:

Design is correct because this phase translates approved business and functional requirements into detailed system specifications that developers can build and testers can validate. An IS auditor should expect control requirements to be embedded in these specifications, including authentication and authorization rules, input validation, processing controls, audit logging, error handling, segregation-of-duties logic, interface controls, and requirements for protecting data. Specifying controls at this point makes them explicit, traceable to requirements and risks, and capable of being tested before the system is placed into production. It also supports a "security by design" approach: security and control requirements are addressed as integral elements of the solution architecture and detailed design rather than being added after coding or deployment. The design documentation therefore provides key audit evidence that control objectives have been translated into implementable system behavior. NIST describes incorporating security requirements throughout the system development life cycle in Security Considerations in the System Development Life Cycle. ISACA's resources on auditing development and implementation emphasize evaluating controls across the development life cycle; see ISACA Journal: Auditing Agile Development.

QUESTION NO: 11

An IS auditor identifies that a legacy application to be decommissioned in three months cannot meet the security requirements established by the current policy. What is the BEST way (or the auditor to address this issue?

A. Recommend the application be patched to meet requirements.

B. Inform the IT director of the policy noncompliance.

C. Verify management has approved a policy exception to accept the risk.

D. Take no action since the application will be decommissioned in three months.

ANSWER: C

Explanation:

Verify management has approved a policy exception to accept the risk. is the best response because the application remains in operation and therefore remains subject to security risk until it is fully decommissioned. A planned retirement date does not itself remove the organization's responsibility to govern the risk during the remaining period of use. Where compliance with the current security policy is not feasible or proportionate for a short-lived legacy system, management—the appropriate risk owner—should explicitly evaluate and accept the residual risk through a documented, time-bound policy exception.

The auditor's role is to determine whether this exception has been formally authorized at the appropriate management level, records the affected requirements and rationale, identifies the residual risk, has a defined expiration aligned to decommissioning, and includes any practical interim safeguards or monitoring. This provides clear accountability and ensures that the exception does not become an unmanaged or indefinite departure from policy. Governance practices require risk decisions to be made by accountable management and documented in a manner that supports oversight. ISACA's governance guidance is available through COBIT resources. The expectation for authorization, documentation, and ongoing monitoring of risk responses is also consistent with the NIST Risk Management Framework.

QUESTION NO: 12

Which of the following is MOST important for an IS auditor to determine during the detailed design phase of a system development project?

A. Program coding standards have been followed

B. Acceptance test criteria have been developed

C. Data conversion procedures have been establish.

D. The design has been approved by senior management.

ANSWER: B

Explanation:

Acceptance test criteria have been developed is the most important determination because detailed design must translate approved business and control requirements into specific, testable conditions that will later demonstrate whether the delivered system is fit for use. An IS auditor should seek evidence that acceptance criteria are objective, complete, traceable to requirements, and agreed with the business or system owner. This includes criteria for functional processing, interfaces, data integrity, security and access controls, exception handling, performance where relevant, and regulatory or policy obligations. Establishing these criteria during design prevents a project from reaching user acceptance testing without a reliable basis for deciding whether it satisfies its intended requirements. It also supports requirements traceability: the auditor can follow each significant requirement through detailed design and planned test cases to final acceptance evidence. Early definition gives the project team time to design controls and functionality that can actually be tested, rather than attempting to define success after development is substantially complete. This aligns with ISACA's assurance focus on evaluating whether systems development governance and controls support business objectives, and with NIST guidance that requires security and privacy requirements to be incorporated and verified throughout the system development life cycle. See ISACA guidance on auditing SDLC processes and NIST SP 800-64 Rev. 2.

QUESTION NO: 13

Which of the following backup schemes is the BEST option when storage media is limited?

A. Real-time backup

B. Virtual backup

C. Differential backup

D. Full backup

ANSWER: C

Explanation:

Differential backup is the best choice among the available schemes when backup storage media is limited. A differential backup begins with a full backup as its baseline and subsequently copies only data that has changed since that baseline. Consequently, it avoids storing a complete duplicate of all protected data during each backup cycle, conserving media capacity while maintaining a straightforward recovery process. To restore data, operations personnel need the baseline full backup and the most recent differential backup, rather than a long chain of separate backup sets. This provides a practical balance between storage consumption, backup administration, and recoverability. Although the size of each differential backup grows as more changes accumulate, organizations can manage this by scheduling a new full backup at an appropriate interval based on data-change rates and available capacity. Backup and recovery planning should define the backup frequency, retention period, media capacity, and recovery requirements as part of a documented contingency strategy. NIST discusses backup strategies and recovery planning in SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. ISACA also identifies backup and recovery controls as relevant audit and governance subjects in its CISA certification resources.

QUESTION NO: 14

In order to be useful, a key performance indicator (KPI) MUST

A. be approved by management.

B. be measurable in percentages.

C. be changed frequently to reflect organizational strategy.

D. have a target value.

ANSWER: D

Explanation:

A KPI must have a target value because a measurement becomes useful for performance management only when it can be evaluated against an intended level of achievement. The target establishes the expected result, threshold, or desired direction for the indicator. It enables management and process owners to determine whether actual performance is acceptable, whether corrective action is needed, and whether progress is being made toward the related business or governance objective. For example, measuring the percentage of critical vulnerabilities remediated is informative, but specifying a target—such as remediation within an established time frame—turns that measurement into a decision-supporting KPI. Targets should be derived from organizational objectives, risk appetite, regulatory obligations, service commitments, and practical performance baselines. They may be reviewed as strategy or operating conditions evolve, but their essential role is to provide a basis for interpreting the measured result. ISACA's COBIT guidance emphasizes using goals, metrics, and target values to monitor achievement and support governance decisions. See ISACA COBIT resources and the ISACA glossary.

QUESTION NO: 15

Which of the following should be GREATEST concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system?

A. Data conversion was performed using manual processes.

B. Backups of the old system and data are not available online.

C. Unauthorized data modifications occurred during conversion.

D. The change management process was not formally documented

ANSWER: C

Explanation:

Unauthorized data modifications occurred during conversion is the greatest concern because it directly compromises the integrity, completeness, and reliability of information transferred to the new application. Conversion is a critical control point: the migrated records become the opening population on which future processing, reporting, operational decisions, and potentially financial reporting will rely. If changes are made without authorization, there is no assurance that the new system accurately represents approved source data or that the organization can trace and substantiate adjustments. An IS auditor should expect conversion controls that restrict update access, preserve source-to-target reconciliation evidence, log exceptions and corrections, require authorized approval of transformation rules and manual adjustments, and establish accountability through an auditable trail. The issue warrants prompt investigation to identify the affected population, validate the completeness and accuracy of migration results, determine whether improper changes must be reversed, and assess whether the new system can be relied upon. This focus aligns with the integrity objective described in NIST's definition of integrity and the access-control and audit-accountability principles in NIST SP 800-53 Rev. 5.

QUESTION NO: 16

Which of the following should an IS auditor recommend as a PRIMARY area of focus when an organization decides to outsource technical support for its external customers?

A. Align service level agreements (SLAs) with current needs.

B. Monitor customer satisfaction with the change.

C. Minimize costs related to the third-party agreement.

D. Ensure right to audit is included within the contract.

ANSWER: A

Explanation:

Align service level agreements (SLAs) with current needs is the primary focus because the agreement establishes the measurable service commitments that the outsourced support provider must meet on the organization's behalf. Before the transition, management should ensure that service expectations reflect current customer requirements, support channels, coverage periods, response and resolution targets, escalation procedures, availability, reporting, security obligations, and remedies for missed performance targets. Clearly defined, business-aligned service levels provide the foundation for governing the supplier relationship and for evaluating whether outsourced support continues to deliver the intended customer experience and business outcomes.

An IS auditor should emphasize that these terms must be sufficiently specific, measurable, and periodically reviewable. Customer needs, technologies, service volumes, and risk tolerances can change; therefore, the SLA should support ongoing performance oversight and controlled updates rather than merely documenting the provider's initial offering. This focus is consistent with ISACA's guidance that governance over external service providers includes defining requirements, monitoring performance, and managing supplier relationships. See ISACA's COBIT resources and the NIST guidance on cybersecurity supply-chain risk management.

QUESTION NO: 17

When evaluating information security governance within an organization, which of the following findings should be of MOST concern to an IS auditor?

A. The information security department has difficulty filling vacancies

B. An information security governance audit was not conducted within the past year

C. The data center manager has final sign-off on security projects

D. Information security policies are updated annually

ANSWER: C

Explanation:

The data center manager has final sign-off on security projects is the finding of greatest concern because it indicates that approval authority for security investments and priorities may reside with an operational IT manager rather than with appropriate executive management or a business-aligned governance body. Information security governance requires clear accountability, appropriate segregation of duties, and decision-making that considers enterprise-wide risk appetite, regulatory obligations, strategic objectives, and the needs of information owners. A data center manager is likely to have valuable technical and operational input, but that role may have priorities centered on infrastructure availability, cost, and operations. Final approval of security projects should be performed by management with sufficient enterprise authority and accountability for business risk, typically through established governance processes involving senior management and relevant business stakeholders. Concentrating final sign-off in an operational role can weaken independent oversight and lead to security decisions that are not adequately aligned with organizational risk management. ISACA describes governance as ensuring that stakeholder needs are evaluated and that direction and monitoring are established at the enterprise level. NIST likewise emphasizes assigning risk-management roles and responsibilities at appropriate organizational levels. See ISACA COBIT resources and NIST SP 800-37 Rev. 2.

QUESTION NO: 18

When an intrusion into an organization network is deleted, which of the following should be done FIRST?

A. Block all compromised network nodes.

B. Contact law enforcement.

C. Notify senior management.

D. Identify nodes that have been compromised.

ANSWER: D

Explanation:

Identify nodes that have been compromised. is the appropriate first action because effective incident response begins by establishing the scope and impact of the intrusion. The organization needs to determine which hosts, accounts, network segments, applications, and data stores show indicators of compromise. This initial identification supports an informed containment decision: responders can isolate the affected assets while avoiding unnecessary disruption to unaffected business services. It also helps preserve relevant evidence, establish a timeline, identify the likely attack path, and determine whether privileged credentials or critical systems are involved. Incident-response procedures should use available sources such as security alerts, endpoint telemetry, authentication and network logs, and forensic indicators to validate which assets are affected. A clear understanding of compromised nodes enables incident management to apply containment measures in a targeted, risk-based manner and communicate an accurate assessment of the incident's business impact. NIST describes analysis as the activity that validates and investigates incident indications, including determining the incident's scope and impact, before response actions are selected and executed. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and NIST incident-response guidance.

QUESTION NO: 19

Which of the following testing methods is MOST appropriate for assessing whether system integrity has been maintained after changes have been made?

A. Regression testing

B. Unit testing

C. Integration testing

D. Acceptance testing

ANSWER: A

Explanation:

Regression testing is the most appropriate method because it verifies that modifications to a system have not adversely affected existing functions, controls, interfaces, data processing, or previously validated behavior. Maintaining system integrity after a change means more than showing that the newly changed component works: the organization needs evidence that the system as a whole continues to operate reliably and consistently with its established requirements. A regression test suite re-executes relevant previously successful test cases following changes such as code updates, configuration changes, patches, interface changes, or infrastructure upgrades. This helps identify unintended side effects and confirms that critical business processes and automated controls still function as expected. For an IS auditor, evidence of risk-based regression-test planning, test execution, results, defect remediation, retesting, and formal approval provides assurance that change management has adequately protected production integrity. The scope should be proportional to the change's risk and include affected upstream and downstream dependencies, especially for high-impact applications. ISACA emphasizes that testing is an essential change-management control and should demonstrate that changes do not create unintended impacts before implementation. See ISACA Journal: Effective IT Change Management and NIST SP 800-128.

QUESTION NO: 20

An IS auditor is reviewing a data conversion project Which of the following is the auditor's BEST recommendation prior to go-live?

A. Review test procedures and scenarios

B. Conduct a mock conversion test

C. Establish a configuration baseline

D. Automate the test scripts

ANSWER: B

Explanation:

Conduct a mock conversion test is the best recommendation because it provides the most direct, end-to-end evidence that the conversion can be completed reliably before production data and business operations are exposed to go-live risk. A mock conversion rehearses the planned extraction, transformation, loading, reconciliation, exception handling, timing, resource requirements, and rollback or contingency procedures under conditions that closely resemble the actual implementation. It enables the project team to identify data-quality defects, incomplete mappings, volume or performance constraints, and operational handoff issues while there is still time to remediate them. The rehearsal should use representative data and predefined acceptance criteria, including record counts, control totals, financial or other critical data reconciliations, and validation that converted data is complete, accurate, and usable by the target system. Results from the mock conversion also support a better-informed go/no-go decision, since management can assess whether conversion duration fits the approved outage window and whether residual risks are acceptable. This aligns with ISACA's focus on validating implementation readiness and controls before deployment, as described in its system-implementation audit guidance. It also reflects established testing practice to validate migration processes and reconcile outcomes before production release; see the NIST guidance on testing and exercises.

QUESTION NO: 21

Which of the following BEST enables an organization to improve the visibility of end-user computing (EUC) applications that support regulatory reporting?

A. EUC inventory

B. EUC availability controls

C. EUC access control matrix

D. EUC tests of operational effectiveness

ANSWER: A

Explanation:

EUC inventory is the best answer because visibility begins with knowing which end-user computing applications exist, who owns them, what business process and regulatory report each supports, where they are hosted, and their risk classification. A complete, maintained inventory provides the population needed for governance, risk assessment, accountability, and ongoing monitoring. It enables management and audit teams to identify critical spreadsheets, databases, desktop tools, and similar user-developed applications that may otherwise operate outside standard application-management processes. For EUCs supporting regulatory reporting, the inventory can also record data sources, key calculations, dependencies, change history, and required controls, allowing the organization to prioritize oversight according to reporting impact and risk. This aligns with COBIT's emphasis on managing information and technology assets through defined ownership, lifecycle practices, and control activities. It also supports regulatory expectations that firms identify and maintain an appropriate inventory of material models and related tools used in decision-making or reporting. Once the EUC population is visible and classified, the organization can apply proportionate access, availability, testing, and change-management controls. See ISACA's COBIT resources and the Bank of England's model risk-management principles.

QUESTION NO: 22

A company has implemented an IT segregation of duties policy. In a role-based environment, which of the following roles may be assigned to an application developer?

A. IT operator

B. System administration

C. Emergency support

D. Database administration

ANSWER: C

Explanation:

Emergency support may be assigned to an application developer because it is an exceptional, temporary role intended to restore service or address a critical incident when normal support personnel are unavailable or cannot resolve the issue in the required timeframe. This access should be granted through a controlled break-glass process: it must be authorized, limited to the specific emergency and minimum necessary privileges, time-bound, fully logged, and subject to prompt independent review after the event. These safeguards allow the organization to maintain availability while retaining accountability and detecting any inappropriate changes made during emergency activity. In a role-based environment, the developer's normal access remains separate from operational production responsibilities; emergency access is not a standing operational entitlement. NIST's separation-of-duties control recognizes that conflicting duties must be separated, while access-control processes can support controlled exceptions with accountability. ISACA's COBIT guidance similarly emphasizes managed access, authorization, monitoring, and review as governance measures for protecting enterprise information and technology. See NIST CSF separation of duties guidance and ISACA COBIT resources.

QUESTION NO: 23

Which of the following tests would provide the BEST assurance that a health care organization is handling patient data appropriately?

A. Compliance with action plans resulting from recent audits

B. Compliance with local laws and regulations

C. Compliance with industry standards and best practice

D. Compliance with the organization's policies and procedures

ANSWER: B

Explanation:

Compliance with local laws and regulations provides the best assurance because these requirements establish the mandatory, enforceable baseline for the collection, use, disclosure, retention, security, and protection of patient data in the relevant jurisdiction. Health care organizations must handle protected health information in accordance with applicable legal obligations, such as privacy, confidentiality, security, breach-notification, and patient-rights requirements. An audit test that evaluates compliance against those obligations directly assesses whether the organization is meeting the authoritative criteria that govern appropriate handling of patient information. For example, in the United States, the HIPAA Privacy Rule defines permitted uses and disclosures and safeguards individuals' rights over protected health information, while the HIPAA Security Rule requires administrative, physical, and technical safeguards for electronic protected health information. A well-designed compliance test maps relevant legal and regulatory requirements to evidence such as access controls, authorization records, privacy notices, incident records, retention practices, and monitoring results. This produces assurance based on externally imposed obligations and supports accountability to regulators, patients, and other stakeholders. Applicable requirements vary by location, so the auditor should identify the laws and regulations governing the organization's operations and the patient data involved. See the HHS HIPAA Privacy Rule and HHS HIPAA Security Rule.

QUESTION NO: 24

A now regulation requires organizations to report significant security incidents to the regulator within 24 hours of identification. Which of the following is the IS auditors BEST recommendation to facilitate compliance with the regulation?

A. Establish key performance indicators (KPIs) for timely identification of security incidents.

B. Engage an external security incident response expert for incident handling.

C. Enhance the alert functionality of the intrusion detection system (IDS).

D. Include the requirement in the incident management response plan.

ANSWER: D

Explanation:

Including the requirement in the incident management response plan is the best recommendation because a regulatory reporting deadline is primarily a governance, process, and coordination requirement. The plan should explicitly define what constitutes a significant incident, when the 24-hour reporting clock begins, the escalation path, accountable owners, required evidence, notification content, approval procedures, and contact details for the regulator. It should also establish procedures for maintaining records that demonstrate the organization met the reporting obligation and for testing the process through exercises. Embedding these items in the response plan turns the regulatory obligation into a repeatable operational procedure that can be executed under the time pressure of an actual incident. It also ensures that security, legal, compliance, management, and communications personnel understand their responsibilities and can act without delaying notification. NIST's incident-response guidance identifies reporting and information sharing as key incident-response activities and emphasizes documenting response procedures and roles. Its updated incident-response publication further integrates response activities into organizational cybersecurity risk management. See NIST SP 800-61 Revision 3 and NIST Cybersecurity Framework 2.0.

QUESTION NO: 25

IS management has recently disabled certain referential integrity controls in the database management system (DBMS) software to provide users increased query performance. Which of the following controls will MOST effectively compensate for the lack of referential integrity?

A. More frequent data backups

B. Periodic table link checks

C. Concurrent access controls

D. Performance monitoring tools

ANSWER: B

Explanation:

Periodic table link checks are the most effective compensating control because they directly test the relationship conditions that referential integrity constraints would otherwise enforce continuously. Referential integrity requires that a foreign-key value in a dependent table correspond to an existing primary or unique-key value in the related parent table, except where a null value is permitted. When those constraints are disabled, invalid or orphaned relationships can be introduced through inserts, updates, data loads, interfaces, or application defects. A periodic link-check process can compare related key values, identify orphan records and other relationship exceptions, produce an exception report, and enable timely correction or escalation by data owners. The check should run at a frequency based on transaction volume, data criticality, and the business impact of inaccurate relationships; high-risk databases may need frequent automated validation. It should also be controlled through documented criteria, retained results, assigned remediation responsibility, and follow-up to confirm that exceptions are resolved. This approach provides detective assurance specifically over the integrity risk created by disabling the constraints. Oracle describes foreign keys and their role in enforcing relationships in its data-integrity documentation; PostgreSQL likewise explains referential integrity through foreign-key constraints.

QUESTION NO: 26

Which of the following would MOST likely impair the independence of the IS auditor when performing a post-implementation review of an application system?

A. The IS auditor provided consulting advice concerning application system best practices.

B. The IS auditor participated as a member of the application system project team, but did not have operational responsibilities.

C. The IS auditor designed an embedded audit module exclusively for auditing the application system.

D. The IS auditor implemented a specific control during the development of the application system.

ANSWER: D

Explanation:

The IS auditor implemented a specific control during the development of the application system. This most likely impairs independence because the subsequent post-implementation review would require the auditor to assess the design, operation, and effectiveness of a control the auditor personally implemented. This creates a self-review threat: the auditor may be perceived as evaluating and defending their own work rather than providing an impartial assessment. Independence must exist both in fact and appearance, so even an objectively performed review may lack credibility if stakeholders reasonably believe that the auditor has an interest in validating a control they put into production.

Implementation is also a management responsibility rather than an assurance activity. An IS auditor may provide independent advice or identify control considerations, but responsibility for selecting, configuring, and implementing controls should remain with management or the project team. Preserving this separation allows the auditor to evaluate whether management's implementation achieved the intended control objectives without having to audit their own decisions or work product. ISACA's professional ethics framework requires members to support appropriate standards and procedures for the effective governance and management of information systems. Its guidance on auditor independence further emphasizes avoiding roles that compromise objective assurance. See ISACA's Code of Professional Ethics and its discussion of auditor independence and objectivity.

QUESTION NO: 27

Demonstrated support from which of the following roles in an organization has the MOST influence over information security governance?

A. Chief information security officer (CISO)

B. Information security steering committee

C. Board of directors

D. Chief information officer (CIO)

ANSWER: C

Explanation:

Board of directors is correct because information security governance is an enterprise governance responsibility requiring direction and oversight from the organization's highest governing body. The board establishes the tone at the top, ensures that security is aligned with business objectives and risk appetite, approves or oversees key policies and strategic investments, and holds executive management accountable for managing information-security risk. Visible board support gives the security program enterprise-wide authority and helps ensure that security requirements are incorporated into strategy, funding, risk management, and organizational priorities rather than treated solely as a technical concern. ISACA's governance guidance identifies the governing body as responsible for evaluating stakeholder needs, setting direction through priorities and decision making, and monitoring performance and compliance. This authority makes demonstrated board-level commitment the most influential support for effective information security governance. The board may delegate implementation and day-to-day management to executives and security leaders, but governance accountability remains at the governing-body level. See ISACA's COBIT framework resources and the NIST Cybersecurity Framework, which describes governance as an organizational responsibility for establishing and monitoring cybersecurity risk-management strategy, expectations, and policy.

QUESTION NO: 28

Which of the following provides the MOST useful information for performing a business impact analysis (B1A)?

A. inventory of relevant business processes

B. Policies for business procurement

C. Documentation of application configurations

D. Results of business resumption planning efforts

ANSWER: A

Explanation:

An inventory of relevant business processes provides the most useful starting information for a business impact analysis because the analysis is fundamentally business-process focused. It establishes what work the organization performs, which processes deliver critical products or services, the owners and users of those processes, and the interdependencies required for them to operate. Using this inventory, management and business process owners can assess the consequences of an interruption over time, including financial, operational, legal, regulatory, customer, and reputational impacts. They can then establish recovery priorities and continuity requirements, such as maximum acceptable downtime and recovery time objectives. A complete process inventory also helps ensure that the analysis covers all significant activities rather than focusing prematurely on individual applications, infrastructure components, or technical configurations. Technical resources and recovery plans may subsequently be mapped to the prioritized processes, but understanding the business processes first is essential to determining what must be recovered and in what order. NIST describes the BIA as identifying and prioritizing information systems and components supporting critical mission/business processes; see NIST SP 800-34 Rev. 1. ISACA's continuity guidance similarly emphasizes determining business impacts and recovery requirements through business-oriented analysis; see ISACA Journal: Business Impact Analysis.

QUESTION NO: 29

A third-party consultant is managing the replacement of an accounting system. Which of the following should be the IS auditor's GREATEST concern?

A. Data migration is not part of the contracted activities.

B. The replacement is occurring near year-end reporting

C. The user department will manage access rights.

D. Testing was performed by the third-party consultant

ANSWER: B

Explanation:

The replacement is occurring near year-end reporting is the greatest concern because the accounting system directly supports the completeness, accuracy, timeliness, and auditability of financial reporting. A conversion close to the reporting cutoff substantially increases the risk that unresolved defects, incomplete reconciliations, incorrect opening balances, interface failures, or processing differences will affect the financial close. It also reduces the time available to perform controlled cutover activities, validate converted data, conduct user acceptance, reconcile key accounts, and establish reliable evidence for management's financial-reporting assertions.

An IS auditor should expect the project to use formal change and release controls, a detailed cutover and rollback plan, defined reconciliation procedures, documented approval to place the system into production, and heightened monitoring through the first reporting cycle. Where a year-end deployment cannot be deferred, management should explicitly assess and accept the residual risk and ensure that contingency procedures can support timely, accurate reporting. This concern is especially significant because financial reporting deadlines are fixed; operational remediation after an unsuccessful conversion may not occur quickly enough to prevent reporting errors or delays. COBIT emphasizes managing change and ensuring that solutions meet business requirements while risks are controlled: ISACA COBIT resources. ISACA's audit resources also emphasize risk-based audit planning and assurance over critical business processes: ISACA audit and assurance standards guidance.

QUESTION NO: 30

Which of the following provides the MOST assurance of the integrity of a firewall log?

A. The log is reviewed on a monthly basis.

B. Authorized access is required to view the log.

C. The log cannot be modified.

D. The log is retained per policy.

ANSWER: C

Explanation:

The log cannot be modified provides the most assurance of firewall-log integrity because integrity means that recorded events remain complete, accurate, and protected from unauthorized or undetected alteration after they are generated. An immutable log preserves the original audit trail, enabling an IS auditor or incident responder to rely on the log as dependable evidence of firewall activity, including allowed connections, denied traffic, rule changes, and administrative events. Technical mechanisms supporting this objective can include append-only storage, write-once-read-many media, cryptographic hashing or signing, centralized remote logging, and tightly controlled log-management processes. The essential assurance is that entries cannot be changed or deleted in a manner that compromises their evidential reliability. ISACA identifies protection of log information from tampering and unauthorized access as a core logging and monitoring concern, while NIST guidance emphasizes protecting audit information and audit tools from unauthorized modification and deletion. See ISACA's guidance on effective security log management and NIST SP 800-92: Guide to Computer Security Log Management.

QUESTION NO: 31

Afire alarm system has been installed in the computer room The MOST effective location for the fire alarm control panel would be inside the

A. computer room closest to the uninterruptible power supply (UPS) module

B. computer room closest to the server computers

C. system administrators office

D. booth used by the building security personnel

ANSWER: D

Explanation:

The most effective location is the *booth used by the building security personnel*. A fire alarm control panel is the point from which alarm conditions are displayed, acknowledged, investigated, and escalated. Locating it with security personnel supports prompt, continuous response because this function is commonly staffed or monitored around the clock. Security personnel can immediately initiate established emergency procedures, notify the fire service and facilities teams, direct responders, and control access to the affected area.

Placing the panel outside the computer room also improves accessibility during an incident. A developing fire, smoke release, suppression-agent discharge, loss of visibility, or restricted access may make entry to the computer room unsafe or impractical. Responders must be able to see the alarm status and operate the panel without first entering the hazard area. This location also helps preserve centralized incident coordination, ensuring that alarms are acted on even when information technology personnel are not present. Fire-alarm control equipment should be located where it is readily accessible to authorized personnel and where the alarm can be promptly managed as part of the building's emergency response process. See the NFPA 72 fire alarm and signaling code overview and the CISA physical security guidance.

QUESTION NO: 32

Which of the following should be an IS auditor's PRIMARY focus when evaluating the response process for cyber crimes?

A. Communication with law enforcement

B. Notification to regulators

C. Root cause analysis

D. Evidence collection

ANSWER: D

Explanation:

Evidence collection is the primary focus because an effective cybercrime response must preserve information that can establish what occurred, when it occurred, which systems and accounts were involved, and how the incident affected the organization. An IS auditor should assess whether procedures identify relevant evidence sources, such as logs, disk images, network captures, cloud records, and volatile system data, and whether personnel can collect that evidence promptly without altering it unnecessarily.

The auditor should also verify that the response process protects evidentiary integrity through documented handling procedures, secure storage, access controls, time synchronization, hashing where appropriate, and a complete chain of custody. These measures support the reliability and admissibility of evidence if the incident leads to internal disciplinary action, litigation, insurance claims, regulatory investigation, or criminal prosecution. They also enable a defensible technical investigation and reliable conclusions about the incident. NIST incident-handling guidance identifies evidence gathering and preservation as essential activities during incident analysis and recovery. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.

QUESTION NO: 33

Which of the following presents the GREATEST challenge to the alignment of business and IT?

A. Lack of chief information officer (CIO) involvement in board meetings

B. Insufficient IT budget to execute new business projects

C. Lack of information security involvement in business strategy development

D. An IT steering committee chaired by the chief information officer (CIO)

ANSWER: A

Explanation:

Lack of chief information officer (CIO) involvement in board meetings presents the greatest challenge because business–IT alignment is fundamentally a governance responsibility that depends on effective communication and decision-making between the board, executive management, and IT leadership. Board-level discussions establish strategic direction, risk appetite, investment priorities, performance expectations, and oversight requirements. Without CIO participation in those discussions, the board may not receive timely, practical insight into technology capabilities, constraints, dependencies, cyber risk, and the implications of strategic decisions for the enterprise architecture and IT portfolio.

Conversely, the CIO may not fully understand evolving business priorities, board concerns, or the rationale behind strategic choices. This disconnect can cause IT plans, investments, delivery priorities, and risk management activities to diverge from enterprise objectives. Meaningful CIO involvement enables technology to be considered as a strategic business enabler rather than solely as an operational support function. It also supports informed board oversight of enterprise information and technology and facilitates accountability for value realization. ISACA's COBIT framework identifies alignment of IT-related goals with enterprise goals as central to governance and management of information and technology. See ISACA COBIT resources and ISACA's discussion of IT governance and the board's role.

QUESTION NO: 34

An organization allows employees to retain confidential data on personal mobile devices. Which of the following is the BEST recommendation to mitigate the risk of data leakage from lost or stolen devices?

A. Require employees to attend security awareness training.

B. Password protect critical data files.

C. Configure to auto-wipe after multiple failed access attempts.

D. Enable device auto-lock function.

ANSWER: C

Explanation:

Configure to auto-wipe after multiple failed access attempts is the best recommendation because it provides a direct, device-enforced safeguard against unauthorized access when a mobile device is lost or stolen. After a defined number of unsuccessful authentication attempts, the device removes its protected data or returns to a secure factory state. This limits the opportunity for an individual in possession of the device to repeatedly guess or systematically attack the access credential and then obtain confidential organizational information.

For personally owned devices that retain organizational data, this control should be implemented through mobile device management or an enterprise mobility management solution, with clear enrollment and data-handling requirements. The organization should define an appropriate failed-attempt threshold and ensure that corporate data is securely managed, while accounting for the practical impact of a wipe on a personal device. NIST identifies device lock, authentication, and mechanisms for securely deleting data as important mobile-device security controls. A wipe policy is particularly valuable because it acts automatically when the device cannot be recovered promptly by the organization. See NIST SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices and NIST Privacy Framework and Cybersecurity Framework resources.

QUESTION NO: 35

An IS auditor finds that capacity management for a key system is being performed by IT with no input from the business The auditor's PRIMARY concern would be:

A. failure to maximize the use of equipment

B. unanticipated increases in business capacity needs.

C. cost of excessive data center storage capacity

D. impact to future business project funding.

ANSWER: B

Explanation:

Unanticipated increases in business capacity needs is the primary concern because capacity management must be driven by current and anticipated business demand, not solely by technical measures of infrastructure utilization. Business stakeholders provide essential information about strategic plans, such as market expansion, new products, acquisitions, seasonal activity, regulatory initiatives, and projected transaction-volume changes. Without this input, IT may forecast demand based only on historical system trends. That approach can leave a key system unable to support material changes in workload when the business needs them, creating a risk to service availability, performance, and the organization's ability to execute its plans. Effective capacity management therefore includes regular communication with business representatives, demand forecasting, and translating expected business activity into measurable resource requirements. This supports the COBIT principle that enterprise objectives should drive technology-related planning and management. ISACA's COBIT resources are available at ISACA COBIT Resources. Capacity management also supports the service-management practice of ensuring that services have sufficient capacity and performance to meet agreed business requirements; see PeopleCert ITIL information.

QUESTION NO: 36

Which of the following BEST guards against the risk of attack by hackers?

A. Tunneling

B. Encryption

C. Message validation

D. Firewalls

ANSWER: D

Explanation:

Firewalls best guard against hacker attacks because they are a preventive network security control designed to enforce an organization's access-control policy at the boundary between networks or security zones. A properly configured firewall examines inbound and outbound traffic against defined rules, allowing only authorized services, protocols, source/destination addresses, and connection states. This reduces the externally reachable attack surface and blocks many unauthorized attempts to access internal systems before those attempts reach the target hosts. Modern next-generation firewalls can also apply application-aware rules, inspect traffic more deeply, and use threat-intelligence or intrusion-prevention capabilities to identify known malicious activity. Their effectiveness depends on a restrictive default posture, disciplined rule administration, logging and monitoring, timely updates, and placement within a layered defense architecture. NIST describes firewalls as controls that mediate traffic between networks with differing security postures and enforce policy governing permitted communications. This direct control of network access makes Firewalls the strongest choice for guarding against hacker attacks. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and CISA Cyber Threats and Advisories.

QUESTION NO: 37

A month after a company purchased and implemented system and performance monitoring software, reports were too large and therefore were not reviewed or acted upon The MOST effective plan of action would be to:

A. evaluate replacement systems and performance monitoring software.

B. restrict functionality of system monitoring software to security-related events.

C. re-install the system and performance monitoring software.

D. use analytical tools to produce exception reports from the system and performance monitoring software

ANSWER: D

Explanation:

Using analytical tools to produce exception reports from the system and performance monitoring software is the most effective action because it converts an excessive volume of monitoring output into focused, actionable information. Monitoring is valuable only when responsible personnel can review the results promptly, recognize conditions that exceed defined thresholds or baselines, and initiate appropriate response or escalation. Exception reporting allows the organization to retain broad monitoring coverage while prioritizing unusual performance conditions, failures, capacity issues, and other events that require attention. This approach addresses the underlying operational problem—unmanageable report volume—without discarding useful monitoring capabilities or replacing a recently implemented solution. It should be supported by documented thresholds, appropriate report recipients, reporting frequency, and periodic tuning to ensure exceptions remain meaningful as the environment changes. NIST guidance on log management similarly emphasizes analysis, prioritization, and automated tools to help organizations handle large quantities of event data and identify significant events efficiently. This supports timely operational oversight and makes monitoring information usable for management and technical teams. See NIST SP 800-92, Guide to Computer Security Log Management and ISACA's CISA certification overview.

QUESTION NO: 38

An IS auditor notes that several employees are spending an excessive amount of time using social media sites for personal reasons. Which of the following should the auditor recommend be performed FIRST?

A. Implement a process to actively monitor postings on social networking sites.

B. Adjust budget for network usage to include social media usage.

C. Use data loss prevention (DLP) tools on endpoints.

D. implement policies addressing acceptable usage of social media during working hours.

ANSWER: D

Explanation:

Implement policies addressing acceptable usage of social media during working hours is the appropriate first recommendation because management must first establish the expected standard of employee behavior and communicate it clearly. An acceptable-use policy defines whether, when, and to what extent personal social-media use is permitted during work time, as well as responsibilities, exceptions, enforcement, and consequences for noncompliance. This provides the governance basis for consistent management action and for any later technical controls or monitoring activities. The policy should be approved by appropriate management, made available to personnel, acknowledged where required, and supported through awareness training. It should also align with broader organizational requirements for internet use, information security, privacy, human resources, and applicable law. Once the rule is defined, management can assess whether technical measures are proportionate and can monitor compliance in a manner that is transparent and authorized. This control sequence supports accountability: policy sets the required behavior, awareness enables employees to understand it, and monitoring or enforcement can subsequently evaluate and address violations. ISACA describes policies as management-approved directives that establish requirements and guide organizational behavior; see ISACA Journal: Information Security Policy—What Does It Really Mean?. For practical acceptable-use policy guidance, see the SANS Information Security Policy Templates.

QUESTION NO: 39

Which of the following security measures will reduce the risk of propagation when a cyberattack occurs?

A. Perimeter firewall

B. Data loss prevention (DLP) system

C. Web application firewall

D. Network segmentation

ANSWER: D

Explanation:

Network segmentation is the security measure that most directly reduces the risk of attack propagation. It divides an enterprise network into separate zones or segments based on business function, system sensitivity, trust level, or operational requirements. Security controls between segments, such as firewalls, access control lists, and tightly defined communication rules, restrict which systems and services can communicate across boundaries. If an attacker compromises a device or workload in one segment, these controls limit lateral movement to other segments and help contain malware, ransomware, or unauthorized access within a smaller portion of the environment.

Effective segmentation applies least-privilege principles to network connectivity: only required traffic between defined sources, destinations, ports, and protocols should be permitted. Critical assets, such as identity infrastructure, payment systems, industrial control systems, and sensitive data repositories, can therefore be isolated from general user networks and from one another. This containment improves resilience and also gives incident responders clearer boundaries for investigation, isolation, and recovery. NIST identifies network segmentation as a means of restricting communications and limiting the impact of security incidents; see NIST SP 800-41 Rev. 1. CISA also recommends segmentation to limit lateral movement and ransomware impact in its StopRansomware Guide.

QUESTION NO: 40

An organization has established hiring policies and procedures designed specifically to ensure network administrators are well qualified Which type of control is in place?

A. Detective

B. Compensating

C. Corrective

D. Directive

ANSWER: D

Explanation:

Directive is correct because the organization has established formal hiring policies and procedures that prescribe how hiring personnel are to select network administrators. Directive controls guide and influence behavior by communicating required practices, responsibilities, and decision criteria. Here, the policies and procedures direct the hiring process toward an intended security outcome: placing competent, suitably qualified individuals in privileged administrative roles. Qualified network administrators are important because their responsibilities commonly include configuring infrastructure, managing access, and maintaining security-sensitive systems. This makes clear personnel requirements an essential governance mechanism for reducing risk before administrative access is granted. ISACA's glossary describes controls and governance terminology used to establish and guide appropriate organizational practices; see the ISACA Glossary. Personnel-security guidance also recognizes that organizations should screen individuals and apply appropriate criteria before authorizing them to occupy sensitive positions. NIST's Personnel Security control family provides related guidance on personnel screening and role suitability in NIST SP 800-53, Rev. 5. The documented hiring requirements therefore function as a directive control by establishing and communicating the expected method for obtaining qualified administrators.

QUESTION NO: 41

An IS auditor is reviewing a bank's service level agreement (SLA) with a third-party provider that hosts the bank's secondary data center, which of the following findings should be of GREATEST concern to the auditor?

A. The recovery time objective (RTO) has a longer duration than documented in the disaster recovery plan (DRP).

B. The SLA has not been reviewed in more than a year.

C. Backup data is hosted online only.

D. The recovery point objective (RPO) has a shorter duration than documented in the disaster recovery plan (DRP).

ANSWER: A

Explanation:

The recovery time objective (RTO) has a longer duration than documented in the disaster recovery plan (DRP) is the greatest concern because it creates a direct, material gap between the bank's approved recovery requirement and the contracted capability of the provider operating the secondary data center. The RTO defines the maximum acceptable time for restoring a service after a disruption. If the provider's SLA permits a longer recovery period, the bank cannot rely on that provider to meet its own DRP commitments during an actual disaster. This exposes critical banking operations, customers, regulatory obligations, and business continuity objectives to an unacceptable interruption risk.

For a third-party-hosted recovery site, the SLA must contain service commitments that support—not conflict with—the bank's business impact analysis and recovery strategy. The auditor should expect the contractual RTO, supporting capacity, recovery procedures, testing requirements, escalation processes, and reporting measures to be aligned with the DRP. NIST explains that recovery objectives should be established based on system criticality and used to guide contingency planning and recovery capabilities. The FFIEC also emphasizes that financial institutions remain responsible for managing business continuity risks arising from third-party service providers. See NIST SP 800-34 Rev. 1 and the FFIEC Business Continuity Management Handbook.

QUESTION NO: 42

When auditing the closing stages of a system development protect which of the following should be the MOST important consideration?

A. Control requirements

B. Rollback procedures

C. Functional requirements documentation

D. User acceptance test (UAT) results

ANSWER: D

Explanation:

User acceptance test (UAT) results are the most important consideration at the closing stage because they provide the formal, business-led evidence that the delivered system is ready for production use. UAT confirms that representative users have tested end-to-end business processes and that the system meets the approved business and functional requirements in the environment intended for operation. For an IS auditor, the key evidence includes documented test scenarios and expected results, actual results, logged defects and their disposition, retesting evidence where needed, formal user/business-owner sign-off, and approval of any residual risks or exceptions. This evidence demonstrates that accountability for accepting the solution rests with the business owner rather than solely with the development team. It also supports the decision to close the project or release it into production, since acceptance establishes that the organization can rely on the system to support its intended processes. ISACA's terminology resources emphasize the importance of controls and assurance throughout system development, while NIST's system development life-cycle guidance identifies acceptance testing as a critical activity before operational deployment. See the ISACA Glossary and NIST SP 800-64 Revision 2.

QUESTION NO: 43

The PRIMARY benefit of automating application testing is to:

A. provide test consistency.

B. provide more flexibility.

C. replace all manual test processes.

D. reduce the time to review code.

ANSWER: A

Explanation:

The primary benefit of automating application testing is to **provide test consistency.** Automated tests execute the same defined steps, use the same test data and expected results, and apply the same pass/fail criteria each time they run. This repeatability is particularly valuable for regression testing, where an organization must repeatedly verify that application changes, patches, or releases have not adversely affected functions that previously worked. Consistent execution makes test results more reliable, comparable across releases, and easier for auditors and stakeholders to evaluate.

Automation can also accelerate execution and permit more frequent testing, but those outcomes stem from the ability to run standardized test scripts repeatedly. Effective automated testing requires controlled test cases, reliable expected outcomes, and appropriate maintenance when application requirements change. These characteristics support a repeatable testing process and strengthen evidence that required functionality was tested consistently. The International Software Testing Qualifications Board describes automated testing as the use of tools to execute tests and compare actual with expected outcomes; repeatable execution is central to that purpose. See the ISTQB definition of test automation and the NIST guide to software assurance.

QUESTION NO: 44

Which of the following is MOST important to verify when determining the completeness of the vulnerability scanning process?

A. The organization's systems inventory is kept up to date.

B. Vulnerability scanning results are reported to the CISO.

C. The organization is using a cloud-hosted scanning tool for Identification of vulnerabilities

D. Access to the vulnerability scanning tool is periodically reviewed

ANSWER: A

Explanation:

The organization's systems inventory is kept up to date is the most important verification because vulnerability-scanning completeness begins with complete and accurate scan scope. An organization cannot demonstrate that all relevant assets are scanned unless it has a current inventory identifying the systems that exist, their ownership, location or environment, technical characteristics, and status. The inventory provides the authoritative population against which the auditor or security team can reconcile scanner targets and scan coverage. This helps identify unmanaged devices, newly deployed systems, retired assets that should be removed from scope, cloud workloads, and systems that may require authenticated or specialized scanning. A current inventory also supports risk-based scan scheduling by enabling assets to be classified according to criticality and exposure. NIST control CM-8 requires organizations to develop, document, review, and update an inventory of system components, including an accurate and current representation of the system. NIST's technical guide for security testing further emphasizes identifying systems and targets as part of planning vulnerability assessments. Therefore, validating that the systems inventory is current is the foundational audit step for determining whether the vulnerability scanning process covers the full intended asset population. See NIST SP 800-53 CM-8 and NIST SP 800-115.

QUESTION NO: 45

An IS auditor has been tasked to review the processes that prevent fraud within a business expense claim system. Which of the following stakeholders is MOST important to involve in this review?

A. Information security manager

B. Quality assurance (QA) manager

C. Business department executive

D. Business process owner

ANSWER: D

Explanation:

The **Business process owner** is the most important stakeholder because this role is accountable for the design, operation, performance, and ongoing improvement of the expense-claim process. Preventive fraud controls are embedded in the business workflow—for example, approval routing, segregation of duties, spending limits, receipt validation, exception handling, and monitoring. The process owner can explain how these controls are intended to operate, identify process-specific fraud risks and control gaps, provide access to relevant procedures and records, and confirm whether corrective actions are practical and can be sustained in day-to-day operations.

From an IS audit perspective, involving the accountable owner supports clear ownership of risk treatment and remediation. The auditor remains independent and evaluates whether controls are appropriately designed and operating effectively, while the process owner is responsible for managing the process and implementing needed improvements. This aligns with COBIT's governance and management concepts, which emphasize assigning clear responsibility and accountability for business processes, controls, and risk-related objectives. ISACA's COBIT resources are available at ISACA COBIT. Additional fraud-risk-management guidance emphasizing business-process ownership and control responsibility is available from COSO's Fraud Risk Management Guide.

QUESTION NO: 46

Which of the following is the BEST way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster?

A. Prepare detailed plans for each business function.

B. Involve staff at all levels in periodic paper walk-through exercises.

C. Regularly update business impact assessments.

D. Make senior managers responsible for their plan sections.

ANSWER: B

Explanation:

Involve staff at all levels in periodic paper walk-through exercises. is the best answer because a business continuity plan is effective only when the people responsible for executing it understand their roles, can identify dependencies, and can apply the plan under realistic disruptive conditions. A structured walk-through brings together business process owners, recovery teams, management, and supporting personnel to step through disaster scenarios, validate escalation and communication paths, confirm decision-making authority, and expose procedural gaps before a real event occurs. Including staff at all levels is particularly important because continuity execution depends on operational knowledge as well as executive direction. Periodic exercises also account for changes in personnel, technology, facilities, suppliers, and business priorities. A paper walk-through is a practical, low-risk testing approach that can be conducted frequently and used to refine the plan iteratively. NIST guidance emphasizes that contingency plans must be tested and exercised to validate their effectiveness and identify needed improvements; see NIST Special Publication 800-34 Rev. 1. ISACA similarly identifies testing, training, and exercising as essential components of organizational resilience and continuity capability; see ISACA's business continuity and resilience guidance.

QUESTION NO: 47

Which of the following controls BEST ensures appropriate segregation of duties within an accounts payable department?

A. Restricting program functionality according to user security profiles

B. Restricting access to update programs to accounts payable staff only

C. Including the creators user ID as a field in every transaction record created

D. Ensuring that audit trails exist for transactions

ANSWER: A

Explanation:

Restricting program functionality according to user security profiles best ensures segregation of duties because it is a preventive application-access control that can enforce each employee's authorized role and prohibit incompatible activities. In accounts payable, responsibilities such as maintaining vendor records, entering invoices, approving invoices, releasing payments, and reconciling payment activity should be allocated so that a single individual cannot initiate and complete a transaction cycle without independent involvement. Role-based security profiles can be configured to grant only the functions necessary for a person's assigned responsibilities and to deny conflicting functions. For example, a profile used to enter supplier invoices can be prevented from approving those invoices or generating payment runs. This control operates consistently at the point the transaction is processed, making the separation enforceable rather than dependent solely on subsequent review. Proper design also requires periodic access reviews and prompt profile updates when staff responsibilities change, so the access rules continue to reflect the approved segregation-of-duties matrix. NIST describes role-based access control as assigning permissions to roles and users to roles, supporting controlled authorization management; see NIST's Role-Based Access Control project. This approach also aligns with ISACA's governance emphasis on managing access to information and related technology resources, described in ISACA COBIT resources.

QUESTION NO: 48

Which of the following should be the PRIMARY role of an internal audit function in the management of identified business risks?

A. Establishing a risk appetite

B. Establishing a risk management framework

C. Validating enterprise risk management (ERM)

D. Operating the risk management framework

ANSWER: C

Explanation:

Validating enterprise risk management (ERM) is the primary role because internal audit provides independent, objective assurance that the organization's risk management processes are appropriately designed and operating effectively. This includes evaluating whether material risks have been identified and assessed, whether risk responses align with approved risk appetite and objectives, whether risk information is reported to appropriate governance bodies, and whether controls supporting those responses are effective. Internal audit may also provide advisory insight, but its assurance work must preserve independence from management's risk ownership and day-to-day decision making. By validating ERM, internal audit gives the board and senior management confidence that the overall framework is reliable and that significant business risks are being governed and monitored appropriately. The Institute of Internal Auditors' Three Lines Model identifies management as responsible for managing risk, while internal audit supplies independent assurance. Its Global Internal Audit Standards likewise require internal audit to assess and contribute to the improvement of governance, risk management, and control processes. See the IIA Global Internal Audit Standards and the IIA Three Lines Model.

QUESTION NO: 49

During an IT general controls audit of a high-risk area where both internal and external audit teams are reviewing the same approach to optimize resources?

A. Leverage the work performed by external audit for the internal audit testing.

B. Ensure both the internal and external auditors perform the work simultaneously.

C. Request that the external audit team leverage the internal audit work.

D. Roll forward the general controls audit to the subsequent audit year.

ANSWER: C

Explanation:

Request that the external audit team leverage the internal audit work is the best response because coordination between assurance providers is intended to achieve appropriate coverage while minimizing unnecessary duplication. When internal audit has performed relevant IT general controls testing, the external audit team may consider using that work after assessing its objectivity, competence, quality, scope, and relevance to the external audit objectives. This can reduce repeated testing while still allowing the external audit team to retain responsibility for its audit conclusions and to perform any additional procedures necessary for a high-risk area.

For internal audit, this approach also supports efficient use of resources without compromising its independent assurance role. Meaningful coordination should include sharing the audit scope, control objectives, test procedures, timing, results, identified exceptions, and supporting workpapers as appropriate. The chief audit executive is expected to coordinate with other assurance providers to ensure proper coverage and minimize duplication. The level of external-audit reliance is always determined by the external auditors under their professional requirements, but making internal audit work available and requesting consideration of it is a sound resource-optimization practice. See the IIA's Global Internal Audit Standards and the IAASB's ISA 610 guidance on using internal auditors' work.

QUESTION NO: 50

A data breach has occurred due lo malware. Which of the following should be the FIRST course of action?

A. Notify the cyber insurance company.

B. Shut down the affected systems.

C. Quarantine the impacted systems.

D. Notify customers of the breach.

ANSWER: C

Explanation:

Quarantine the impacted systems is the appropriate first action because immediate containment limits the malware's ability to spread laterally, communicate with command-and-control infrastructure, exfiltrate additional data, or compromise further assets. Quarantine normally means logically isolating affected endpoints or servers from untrusted networks while retaining the systems in a state that permits incident responders to collect volatile information, logs, malware samples, and other evidence needed to determine scope and support recovery. The exact containment method should be selected according to the organization's incident response procedures and operational needs; it may include network isolation, access-control restrictions, or endpoint detection and response isolation. This action should be initiated promptly and coordinated through the incident response process so that business impact, evidence preservation, and the risk of further harm are managed together. NIST's incident-handling guidance identifies containment as a core activity after incident detection and analysis, and emphasizes choosing and implementing containment strategies appropriate to the incident. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and the CISA Cybersecurity Incident Response guidance.

QUESTION NO: 51

The PRIMARY benefit of information asset classification is that it:

A. prevents loss of assets.

B. helps to align organizational objectives.

C. facilitates budgeting accuracy.

D. enables risk management decisions.

ANSWER: D

Explanation:

Information asset classification primarily enables risk management decisions because it establishes the business value, sensitivity, criticality, and handling requirements of information assets. Once an organization knows which assets are public, internal, confidential, regulated, or mission-critical, it can make informed, risk-based decisions about the level of protection required. These decisions include selecting appropriate access controls, encryption, retention periods, backup and recovery capabilities, monitoring, incident-response priorities, and third-party handling requirements. Classification also gives asset owners and control stakeholders a common basis for determining whether residual risk is acceptable and where security investment should be prioritized. In an audit context, classification provides criteria for evaluating whether safeguards are commensurate with the importance of the information and the impact of compromise. This supports the governance principle that controls and resources should be applied proportionately to business risk, rather than uniformly to every asset. ISACA's risk-management guidance emphasizes identifying and assessing risk to support informed treatment decisions, while NIST identifies information classification as a foundation for selecting protections appropriate to impact. See ISACA guidance on enterprise risk management and information security and NIST FIPS 199.

QUESTION NO: 52

Which of the following provides a new IS auditor with the MOST useful information to evaluate overall IT performance?

A. IT value analysis

B. Prior audit reports

C. IT balanced scorecard

D. Vulnerability assessment report

ANSWER: C

Explanation:

IT balanced scorecard is correct because it provides a structured, enterprise-level view of whether IT is delivering the outcomes expected by the organization. Adapted from the balanced-scorecard approach, an IT balanced scorecard translates IT strategy into objectives, performance measures, targets, and initiatives across complementary perspectives such as business contribution, user orientation, operational excellence, and future orientation. This gives a new IS auditor a consolidated basis for assessing performance against approved goals rather than relying on isolated technical, financial, or historical information.

For an overall evaluation, the auditor needs evidence that connects IT activities and service delivery to business value, stakeholder needs, process effectiveness, and capability development. The scorecard supports this by showing both outcome measures and performance drivers, enabling the auditor to identify significant performance trends, gaps against targets, and areas that may warrant further audit work. This alignment with enterprise objectives is consistent with COBIT's focus on governing and managing information and technology to create value while balancing benefits realization, risk optimization, and resource optimization. See ISACA's COBIT resources and the Balanced Scorecard Institute overview.

QUESTION NO: 53

Which of the following would lead an IS auditor to conclude that the evidence collected during a digital forensic investigation would not be admissible in court?

A. The person who collected the evidence is not qualified to represent the case.

B. The logs failed to identify the person handling the evidence.

C. The evidence was collected by the internal forensics team.

D. The evidence was not fully backed up using a cloud-based solution prior to the trial.

ANSWER: B

Explanation:

The logs failed to identify the person handling the evidence is correct because this represents a break in the documented chain of custody. For digital evidence to be admitted, its proponent must be able to establish that the evidence is what it is claimed to be and that it has remained under controlled handling without unauthorized alteration. Chain-of-custody documentation records each transfer, including the identity of the individual releasing or receiving the evidence, the date and time, the purpose of the transfer, and appropriate integrity details such as hashes. If handling logs do not identify the person responsible for possession or transfer, the organization cannot reliably account for who controlled the evidence during that period. This prevents a clear, defensible demonstration of continuity and authenticity and can undermine the evidence's admissibility or evidentiary weight in court. A sound forensic process therefore preserves original evidence, uses documented custody procedures, and maintains complete records from collection through analysis and presentation. NIST's forensic guidance emphasizes maintaining chain-of-custody records and preserving evidence integrity throughout the investigation; see NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. The U.S. Department of Justice also addresses documentation and preservation practices for digital evidence in its Electronic Crime Scene Investigation guide.

QUESTION NO: 54

An IS auditor finds the log management system is overwhelmed with false positive alerts. The auditor's BEST recommendation would be to:

A. establish criteria for reviewing alerts.

B. recruit more monitoring personnel.

C. reduce the firewall rules.

D. fine tune the intrusion detection system (IDS).

ANSWER: D

Explanation:

Fine tune the intrusion detection system (IDS) is the best recommendation because excessive false positives generally indicate that detection logic is not sufficiently aligned to the organization's actual environment, normal traffic patterns, assets, and risk priorities. IDS tuning involves validating alert signatures and rules, establishing appropriate thresholds, suppressing known-benign and duplicate events where justified, maintaining approved exceptions, and baselining legitimate activity. This improves the signal-to-noise ratio so that monitoring personnel can identify, investigate, and escalate genuinely suspicious events promptly.

From an audit perspective, tuning should be a controlled, risk-based process. Changes should be documented, tested, approved, and periodically reviewed to ensure that reducing noise does not create unacceptable detection gaps. The organization should also retain monitoring coverage for high-risk systems and use incident findings to refine rules continuously. NIST notes that continuous monitoring relies on collecting and analyzing security-related information to support risk decisions, while alerting capabilities must provide useful information for response. Guidance on IDS deployment and management likewise emphasizes configuring and tuning detection technologies for the monitored environment. See NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems and NIST SP 800-137, Information Security Continuous Monitoring.

QUESTION NO: 55

The BEST way to determine whether programmers have permission to alter data in the production environment is by reviewing:

A. the access control system's log settings.

B. how the latest system changes were implemented.

C. the access control system's configuration.

D. the access rights that have been granted.

ANSWER: D

Explanation:

the access rights that have been granted. is correct because permissions to alter production data are determined by the effective entitlements assigned to individual programmer accounts, including direct rights, group-derived rights, privileged-role assignments, and any relevant database or application authorization. An auditor should review these granted access rights against the approved access model and the programmer's job responsibilities to establish whether the individual is authorized to perform data changes in production. This directly tests the segregation-of-duties control intended to keep development personnel from making unauthorized production changes.

Effective access reviews should also account for the identity-to-account relationship and the scope of each entitlement, such as update, insert, delete, execute, or administrative permissions. Evidence may include identity and access management entitlement reports, directory group memberships, database roles, application roles, and approved access requests. NIST identifies account management and access enforcement as controls for managing account privileges and enforcing approved authorizations; these principles support reviewing the permissions actually granted to accounts. See NIST SP 800-53 Rev. 5 and the ISACA Journal guidance on identity and access management auditing.

QUESTION NO: 56

Which of the following provides the BEST audit evidence that a firewall is configured in compliance with the organization's security policy?

A. Analyzing how the configuration changes are performed

B. Analyzing log files

C. Reviewing the rule base

D. Performing penetration testing

ANSWER: C

Explanation:

Reviewing the rule base provides the best audit evidence because it directly examines the firewall's implemented access-control logic—the source and destination addresses, services, ports, protocols, actions, rule order, logging settings, and any exceptions. An auditor can map these active rules to the organization's approved security-policy requirements and network-security standards, confirming that permitted traffic has a documented business basis and that prohibited or unauthorized traffic is denied. This is direct evidence of the configuration currently enforcing policy, rather than indirect evidence about supporting processes or observed events. A sound review should include the complete active policy, including default-deny behavior, object definitions, network address translation where relevant, administrative access restrictions, and rules that may be disabled, shadowed, overly broad, expired, or insufficiently logged. The auditor should also reconcile material rules and exceptions to approved change records and validate that the reviewed rule base represents the production configuration. NIST's firewall guidance emphasizes establishing and maintaining firewall policies and rules that enforce the organization's security requirements; see NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy. ISACA also identifies configuration review as a key audit activity for evaluating the effectiveness of technical controls; see ISACA Journal: Configuration Management Audit.

QUESTION NO: 57

What would be an IS auditor's BEST recommendation upon finding that a third-party IT service provider hosts the organization's human resources (HR) system in a foreign country?

A. Perform background verification checks.

B. Review third-party audit reports.

C. Implement change management review.

D. Conduct a privacy impact analysis.

ANSWER: D

Explanation:

Conduct a privacy impact analysis is the best recommendation because an HR system ordinarily processes sensitive, personally identifiable employee information, and hosting it in another country introduces privacy risks that must be evaluated in the context of the organization's specific processing activity. A privacy impact analysis provides a structured way to identify what personal data is collected and transferred, the purposes and legal basis for processing, the jurisdictions involved, applicable employee-data and cross-border transfer requirements, retention arrangements, access by the provider or public authorities, and safeguards needed to reduce risk. It also helps establish whether contractual, technical, and organizational measures are sufficient before or during continued use of the service provider. This recommendation addresses the primary governance and compliance implication of foreign hosting: the organization remains accountable for protecting HR data even when processing is outsourced. Privacy assessments are especially appropriate where processing may create elevated risks to individuals' rights and freedoms, such as large-scale handling of employee records. The European Commission's guidance on data protection impact assessments describes assessing necessity, proportionality, risks, and safeguards: European Commission guidance. Cross-border personal-data transfer safeguards are further addressed in Regulation (EU) 2016/679.

QUESTION NO: 58

Which of the following should be done FIRST when planning a penetration test?

A. Execute nondisclosure agreements (NDAs).

B. Determine reporting requirements for vulnerabilities.

C. Define the testing scope.

D. Obtain management consent for the testing.

ANSWER: D

Explanation:

Obtain management consent for the testing. is the first action because a penetration test intentionally attempts activities that could otherwise be treated as unauthorized access, disruption, or policy violations. Explicit authorization from the appropriate management authority establishes the tester's legal and organizational authority to act and confirms that the organization accepts the engagement at a governance level. This authorization should be documented, identify the sponsoring authority, and provide the basis for subsequently developing the rules of engagement.

Once management has approved the test, the team can formally establish the engagement's scope, systems and locations in scope, permitted testing techniques, operational constraints, emergency contacts, communications and escalation paths, handling of sensitive information, and vulnerability reporting requirements. Confidentiality arrangements, including NDAs where appropriate, can also be completed as part of engagement preparation under the approved testing authority. NIST describes planning as requiring clear authorization and rules of engagement before technical security testing begins; this protects the organization, its personnel, and the testers while ensuring the test supports legitimate business objectives. See NIST SP 800-115, Technical Guide to Information Security Testing and Assessment and ISACA's Penetration Testing: A Practical Approach.

QUESTION NO: 59

An IS auditor is reviewing the installation of a new server. The IS auditor's PRIMARY objective is to ensure that

A. security parameters are set in accordance with the manufacturer s standards.

B. a detailed business case was formally approved prior to the purchase.

C. security parameters are set in accordance with the organization's policies.

D. the procurement project invited lenders from at least three different suppliers.

ANSWER: C

Explanation:

Security parameters are set in accordance with the organization's policies is correct because the auditor's primary concern during server installation is whether the implementation satisfies governance-approved requirements for security, risk management, and internal control. Organizational policies establish the mandatory baseline for matters such as account and privileged-access administration, authentication, system hardening, logging and monitoring, vulnerability and patch management, encryption, network configuration, backup, and exception handling. They translate management's risk appetite and applicable legal, regulatory, and contractual obligations into requirements that can be tested and enforced consistently across the environment. Manufacturer defaults or recommended standards can provide useful technical implementation guidance, but they must be assessed and configured to meet the organization's own approved security requirements rather than being accepted without validation. The auditor should seek evidence that the server was securely configured, that required deviations were formally authorized through an exception process, and that configuration records and testing demonstrate compliance before production use. This focus supports ISACA's principle that security governance and controls should align with enterprise objectives and risk requirements. See ISACA's guidance on security configuration management and NIST's Guide for Security-Focused Configuration Management.

QUESTION NO: 60

Which of the following BEST ensures the quality and integrity of test procedures used in audit analytics?

A. Developing and communicating test procedure best practices to audit teams

B. Developing and implementing an audit data repository

C. Decentralizing procedures and Implementing periodic peer review

D. Centralizing procedures and implementing change control

ANSWER: D

Explanation:

Centralizing procedures and implementing change control best ensures that audit-analytics test procedures remain reliable, repeatable, and defensible. A centralized repository or managed library establishes an authoritative version of each analytic routine, including its purpose, logic, required data, parameters, expected results, and supporting documentation. This enables consistent execution across audit engagements and makes it easier to establish ownership, apply common quality standards, and retain an audit trail of how a procedure was developed and used. Formal change control protects the integrity of those procedures over time: proposed amendments can be documented, risk-assessed, reviewed, approved by an authorized party, tested or validated before release, versioned, and communicated to users. These controls are especially important when procedures are reused, when source systems change, or when analytic logic is updated. Together, centralization and change control provide governance over both the approved baseline and every subsequent modification, supporting the COBIT emphasis on managed processes, accountability, and controlled information assets. See ISACA's COBIT resources and NIST's guidance on configuration change control in SP 800-53 CM-3.

QUESTION NO: 61

An IS auditor discovers that validation controls m a web application have been moved from the server side into the browser to boost performance This would MOST likely increase the risk of a successful attack by.

A. phishing.

B. denial of service (DoS)

C. structured query language (SQL) injection

D. buffer overflow

ANSWER: C

Explanation:

structured query language (SQL) injection is correct because browser-side validation is under the control of the user and cannot be relied on as a security boundary. An attacker can bypass JavaScript validation by modifying browser behavior, intercepting and altering requests with a proxy, or submitting requests directly to the application endpoint without using the browser interface. If the server accepts the resulting input without independently validating it and enforcing parameterized database queries, attacker-supplied input can be interpreted as part of an SQL command. This can permit unauthorized reading, modification, or deletion of database data, depending on the application and database account privileges.

Input validation must therefore be performed on the server, where the application controls enforcement and can apply consistent rules to every request regardless of its source. Server-side validation should be combined with prepared statements or parameterized queries, which separate data values from SQL syntax and provide the primary technical defense against SQL injection. Client-side validation may still be useful for usability and reducing invalid submissions, but it is only a convenience control and must supplement—not replace—server-side protections. OWASP specifically notes that client-side validation can be bypassed and identifies parameterized queries as a key SQL injection prevention measure. See the OWASP Input Validation Cheat Sheet and the OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 62

Which of the following is MOST important for an effective control self-assessment (CSA) program?

A. Determining the scope of the assessment

B. Performing detailed test procedures

C. Evaluating changes to the risk environment

D. Understanding the business process

ANSWER: D

Explanation:

Understanding the business process is most important because a control self-assessment must be grounded in how work is actually performed, how information and assets flow, which objectives the process is intended to achieve, and where risks can prevent those objectives from being met. This understanding enables process owners and participants to identify the controls embedded in day-to-day activities and make meaningful judgments about whether those controls are designed appropriately and operating as intended. It also provides the context needed to connect risks, control activities, accountabilities, and performance measures to the organization’s business objectives. A CSA is a participative assessment technique rather than simply an audit testing exercise; its value depends substantially on informed input from the people who know the process. Clear process understanding therefore supports a focused, credible discussion of risk and control and produces results that management can use to improve governance and internal control. This aligns with COSO’s emphasis on identifying and assessing risks in relation to objectives and designing control activities that address those risks. See the COSO Internal Control guidance and ISACA’s COBIT resources for related governance, process, risk, and control concepts.

QUESTION NO: 63

Providing security certification for a new system should include which of the following prior to the system's implementation?

A. End-user authorization to use the system in production

B. External audit sign-off on financial controls

C. Testing of the system within the production environment

D. An evaluation of the configuration management practices

ANSWER: D

Explanation:

An evaluation of the configuration management practices is correct because security certification requires a structured assessment of whether the system's security controls are properly implemented and will remain in a known, controlled state throughout its lifecycle. Configuration management is fundamental to that assessment: it establishes approved baselines, controls and documents changes, maintains configuration records, and helps ensure that security-relevant components are consistently deployed as designed. Evaluating these practices before implementation provides assurance that unauthorized or unreviewed changes will not undermine the control environment after the system enters service. It also supports repeatable remediation, vulnerability management, and continuing assessment by making the system's hardware, software, settings, and changes traceable to an approved baseline. NIST describes configuration management as a process for establishing and maintaining the integrity of information systems through control of the processes for initializing, changing, and monitoring configurations. See NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems. This activity fits the certification purpose of providing decision makers with reliable evidence concerning security controls and the system's security posture before it is placed into operation. The related control assessment and authorization concepts are detailed in NIST SP 800-37 Rev. 2.

QUESTION NO: 64

To develop meaningful recommendations 'or findings, which of the following is MOST important 'or an IS auditor to determine and understand?

A. Root cause

B. Responsible party

C. impact

D. Criteria

ANSWER: A

Explanation:

Root cause is the most important factor to determine and understand when developing meaningful audit recommendations. A finding describes a condition that deviates from established criteria and may identify resulting or potential impact, but a recommendation should address the underlying reason the condition occurred. Identifying the root cause enables the auditor to propose corrective action that is practical, proportionate, and directed at preventing recurrence rather than merely treating a visible symptom. For example, where inappropriate access exists, the meaningful recommendation depends on whether the underlying cause is ineffective provisioning procedures, an inadequately configured access-control system, unclear ownership, insufficient review, or a lack of staff awareness. Understanding the cause also helps management select an accountable action plan, allocate appropriate resources, and establish measures that demonstrate remediation is sustainable. Audit reporting guidance commonly structures findings around criteria, condition, cause, and effect; this analysis creates the evidence-based connection between the observed issue and a recommendation. ISACA's audit and assurance standards emphasize reporting significant findings and recommendations in a manner that supports corrective action and follow-up. See ISACA's audit reporting guidance and the IIA Global Internal Audit Standards for the importance of communicating causes and recommendations that support effective remediation.

QUESTION NO: 65

Which of the following is the MOST important consideration when evaluating the data retention policy for a global organization with regional offices in multiple countries?

A. The policy aligns with corporate policies and practices.

B. The policy aligns with global best practices.

C. The policy aligns with business goals and objectives.

D. The policy aligns with local laws and regulations.

ANSWER: D

Explanation:

The policy aligns with local laws and regulations because a global retention policy must be implemented in a way that satisfies the mandatory legal requirements applicable in every jurisdiction where the organization collects, processes, stores, or is otherwise subject to rules governing information. Retention obligations are not uniform internationally: privacy laws can require personal data to be retained only for a defined, necessary period, while tax, employment, financial-services, litigation-hold, archival, and sector-specific rules may prescribe minimum retention periods or conditions for disposal. The organization therefore needs a jurisdictional retention schedule that identifies applicable legal requirements, assigns accountable owners, and translates them into operational controls for records classification, storage, legal holds, secure deletion, and evidence of compliance. This is especially important because retaining data too long can breach data-minimization and storage-limitation requirements, whereas deleting it too early can violate recordkeeping duties or impair the organization's ability to respond to regulators, audits, or legal proceedings. For example, the EU General Data Protection Regulation requires personal data to be kept no longer than necessary for its processing purpose, subject to lawful retention needs. A sound global policy establishes a common framework but permits locally required variations. See GDPR, Article 5 and NIST Privacy Framework.

QUESTION NO: 66

Which of the following security risks can be reduced by a property configured network firewall?

A. SQL injection attacks

B. Denial of service (DoS) attacks

C. Phishing attacks

D. Insider attacks

ANSWER: B

Explanation:

Denial of service (DoS) attacks can be reduced by a properly configured network firewall because the firewall can enforce traffic-control rules before unwanted traffic reaches protected systems. For example, it can restrict access to only required ports, protocols, source and destination addresses, and approved services. Many next-generation firewalls also support connection limits, rate limiting, session inspection, SYN-flood protections, and automated blocking of traffic patterns that exceed established thresholds. These controls can reduce the ability of a single source or a limited set of sources to exhaust server resources, consume connection tables, or overwhelm exposed network services. Firewall logging and alerting further support rapid detection and response when abnormal traffic volumes occur. A firewall is therefore an important preventive and detective layer within a defense-in-depth design for availability risks. Its effectiveness depends on a rule base that permits only necessary traffic, is monitored and maintained, and is complemented by capacity planning and upstream provider protections for high-volume attacks. NIST describes firewalls as controls that monitor and control communications at network boundaries in accordance with security policy; see NIST SP 800-41 Rev. 1. Guidance on handling denial-of-service incidents is also available in NIST SP 800-61 Rev. 2.

QUESTION NO: 67

Which of the following is the BEST source of information for an IS auditor to use as a baseline to assess the adequacy of an organization's privacy policy?

A. Historical privacy breaches and related root causes

B. Globally accepted privacy best practices

C. Local privacy standards and regulations

D. Benchmark studies of similar organizations

ANSWER: C

Explanation:

Local privacy standards and regulations are the best baseline because an organization's privacy policy must first meet the mandatory legal and regulatory obligations applicable to its operations, customers, employees, data-processing activities, and jurisdictions. These requirements establish enforceable expectations for such matters as lawful collection and processing, notice and transparency, individual rights, retention, security safeguards, breach notification, cross-border transfers, and accountability. An IS auditor can use the applicable requirements as objective audit criteria, map policy provisions to each obligation, and determine whether the policy is complete, current, and appropriately approved. This approach also recognizes that privacy obligations vary significantly by location and sector; therefore, adequacy cannot be assessed reliably without identifying the specific rules that govern the organization. For example, the European Data Protection Board provides guidance on the application of the EU General Data Protection Regulation, including controller accountability and data-subject rights: EDPB Data Protection Guide. In the United States, the Federal Trade Commission describes privacy and data-security expectations and enforcement considerations: FTC Privacy and Security. These authoritative local obligations provide the primary compliance threshold against which the auditor should assess the policy.

QUESTION NO: 68

Which of the following is the GREATEST benefit of adopting an international IT governance framework rather than establishing a new framework based on the actual situation of a specific organization1?

A. Readily available resources such as domains and risk and control methodologies

B. Comprehensive coverage of fundamental and critical risk and control areas for IT governance

C. Fewer resources expended on trial-and-error attempts to fine-tune implementation methodologies

D. Wide acceptance by different business and support units with IT governance objectives

ANSWER: D

Explanation:

Wide acceptance by different business and support units with IT governance objectives is the greatest benefit because a recognized international framework provides an established, common basis for discussing, governing, and controlling IT. IT governance necessarily involves stakeholders beyond the IT function, including executive management, risk, compliance, audit, security, finance, and business-process owners. A framework that is externally recognized and based on broadly accepted practices helps these groups align around common terminology, governance objectives, control expectations, and accountability structures. This shared foundation reduces debate over whether the governance model itself is credible and enables the organization to focus on tailoring implementation to its own strategy, risk appetite, regulatory environment, and operating model. Frameworks such as COBIT are specifically designed to bridge enterprise governance objectives with IT management practices, facilitating communication and alignment among stakeholders. ISACA describes COBIT as a framework for the governance and management of enterprise information and technology, intended to create value by balancing benefits realization, risk optimization, and resource optimization. Its widespread recognition gives it greater organizational legitimacy than a wholly new internally developed framework. See ISACA's COBIT resource page and ISACA's COBIT framework overview.

QUESTION NO: 69

Which of the following should an organization do to anticipate the effects of a disaster?

A. Define recovery point objectives (RPO)

B. Simulate a disaster recovery

C. Develop a business impact analysis (BIA)

D. Analyze capability maturity model gaps

ANSWER: C

Explanation:

Develop a business impact analysis (BIA) is correct because a BIA systematically identifies critical business processes, the resources and dependencies that support them, and the operational, financial, legal, regulatory, and reputational consequences of an interruption. This analysis enables the organization to anticipate how a disaster would affect business operations over time rather than focusing only on the technical recovery of systems. It establishes the basis for recovery priorities and continuity requirements, including maximum tolerable downtime and the recovery objectives needed to sustain essential services. A well-executed BIA also involves business-process owners, ensuring that impact assessments reflect the organization's actual mission, customer commitments, and obligations. Its results drive practical business continuity and disaster recovery strategies, resource allocation, and recovery-plan design. ISACA's business continuity guidance identifies business impact analysis as a core activity for understanding disruption impacts and determining continuity requirements. NIST likewise describes the BIA as the process used to identify and prioritize information systems and determine the consequences of a disruption. See ISACA's Business Impact Analysis guidance and NIST Business Impact Analysis glossary definition.

QUESTION NO: 70

Which of the following is the MOST effective way to identify exfiltration of sensitive data by a malicious insider?

A. Implement data loss prevention (DLP) software

B. Review perimeter firewall logs

C. Provide ongoing information security awareness training

D. Establish behavioral analytics monitoring

ANSWER: A

Explanation:

Implement data loss prevention (DLP) software is the most effective choice because DLP is designed specifically to discover, classify, monitor, and enforce handling rules for sensitive information as it is used, shared, or transmitted. For insider-related exfiltration, DLP controls can inspect content and context—such as regulated data patterns, document labels, recipients, destination domains, upload channels, removable media use, printing, and cloud sharing—and generate alerts or block policy-violating transfers. This provides direct visibility into an attempted or completed movement of the sensitive data itself, rather than relying only on general network activity or indications of unusual user behavior. Effective DLP deployment starts with a data classification scheme and policies that identify the organization's sensitive data and authorized transfer scenarios. Alerts should be triaged through established incident-response processes, with appropriate tuning to reduce false positives and preserve evidence. NIST's security-control catalog identifies protections for data in transit and boundary protection as important control areas; DLP operationalizes these protections with data-aware inspection and enforcement. See NIST SP 800-53 Rev. 5 and Microsoft Purview Data Loss Prevention documentation.