ISACA CISA Exam Questions

Total Questions: 1400+
Demo Questions: 29
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit: CISA Exam Dumps by Cert Empire

Question: 1

Which of the following is the PRIMARY reason to adopt a capability model?

A: To increase the organization's level of security

B: To guide improvement of organizational processes

C: To decrease the organization's level of risk

D: To ensure compliance with laws and regulation

Correct Answer:

B

Explanation:

The primary purpose of a capability model, such as COBIT or CMMI (Capability Maturity Model Integration), is to provide a structured framework for assessing an organization's current process capabilities and guiding their systematic improvement. These models define different levels of maturity, allowing an organization to benchmark its current state ("as-is") and identify the specific steps needed to reach a more mature, effective, and predictable future state ("to-be"). The core function is the continuous improvement of processes to better achieve organizational objectives.

Why Incorrect Options are Wrong:

A: To increase the organization's level of security: Increasing security is a potential benefit of improving processes, but it is not the primary, overarching purpose of the capability model itself, which focuses on the processes.

C: To decrease the organization's level of risk: Risk reduction is a significant outcome of having more mature and predictable processes, but the model's direct focus is on guiding process improvement, not directly on risk mitigation.

D: To ensure compliance with laws and regulation: While improved processes help achieve compliance, a capability model's scope is broader, focusing on overall process effectiveness, of which compliance is just one aspect.

References:

1. ISACA, COBIT® 2019 Framework: Introduction and Methodology, Page 33. The framework states, "The COBIT performance management (CPM) model is an integral part of the COBIT framework... It allows organizations to measure performance to... support process improvement." This directly links the model to process improvement.

2. Carnegie Mellon University, Software Engineering Institute (SEI). The CMMI model is defined as "a capability improvement framework that provides organizations with the essential elements of effective processes that ultimately improve their performance." This highlights process improvement as the central goal. (Source: https://www.sei.cmu.edu/our-work/cmmi/index.cfm - Note: While the SEI website has evolved, the foundational definition of CMMI as a process improvement model is a core academic and historical fact from the institution).

3. Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, V. (1993). Capability Maturity Model for Software, Version 1.1. (CMU/SEI-93-TR-024). Carnegie-Mellon University. The foundational document for CMM states its purpose is to provide "a framework for organizing these evolutionary steps into five maturity levels that lay successive foundations for continuous process improvement." (Page 1-2).

Question: 2

Which of the following provides the BEST evidence of the effectiveness of an organization s audit quality management procedures?

A: Quality of independent review scores

B: Number of resources dedicated to quality control procedures

C: Quality of auditor performance reviews

D: Number of audits completed within the annual audit plan

Correct Answer:

A

Explanation:

The effectiveness of an audit quality management program is best measured by its outcomes. An independent review, such as a Quality Assurance Review (QAR), provides an objective, external assessment of the audit function's adherence to professional standards (e.g., ISACA's ITAF) and the quality of its work products. The scores and findings from such a review are a direct, evidence-based measure of the quality management procedures' success in achieving their intended purpose, making it the most reliable indicator of effectiveness.

Why Incorrect Options are Wrong:

B: The number of resources is an input metric. A high level of resource allocation does not guarantee that the quality control procedures are effective or producing high-quality results.

C: Auditor performance reviews focus on individual staff competency and development, which is only one component of a quality program and can be subjective. They do not assess the overall system's effectiveness.

D: This measures the efficiency and completion rate of the audit plan, not the quality or effectiveness of the audits performed. An audit function can be efficient but produce low-quality work.

References:

1. ISACA, ITAF: A Professional Practices Framework for IS Audit/Assurance, 4th Edition, Guideline 2401 Quality Assurance. This guideline states that a quality assurance program should include "periodic internal and external quality assessments" to "assess the efficiency

and effectiveness of the IS audit function." The results of these assessments are the primary evidence.

2. ISACA, CISA Review Manual, 27th Edition, Chapter 1: The Process of Auditing Information Systems. The section on Quality Assurance and Improvement Program (QAIP) emphasizes that the program must include both internal and external assessments. The results of these assessments provide assurance that the audit function operates in conformity with standards, which is the definition of effectiveness.

3. The Institute of Internal Auditors (IIA), International Standards for the Professional Practice of Internal Auditing (Standards), Standard 1312: External Assessments. ISACA's standards are aligned with the IIA's. Standard 1312 mandates external assessments at least once every five years by a qualified, independent reviewer. The results provide an opinion on the audit activity's conformance with standards, directly evidencing effectiveness. (Available at: https://www.theiia.org/)

Question: 3

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: Haphazard sampling

B: Attribute sampling

C: Variable sampling

D: Quota sampling

Correct Answer:

B

Explanation:

Attribute sampling is the most appropriate method for compliance testing. This statistical technique is used to determine the rate of occurrence of a specific characteristic (an "attribute") within a population. In this scenario, the auditor is testing whether the control—capturing both an ID number and a photo—is operating effectively. Each log entry either complies (pass) or does not (fail). Attribute sampling allows the auditor to statistically conclude on the effectiveness of the control for the entire population of log entries based on a sample.

Why Incorrect Options are Wrong:

A: Haphazard sampling: This is a non-statistical method that relies on auditor judgment without a structured approach. It does not allow for a statistically valid conclusion about the entire population's compliance rate.

C: Variable sampling: This method is used in substantive testing to estimate a numerical value (e.g., monetary amount), not to test the rate of compliance with a control (a pass/fail test).

D: Quota sampling: This is a non-statistical method that selects a predetermined number of items from subgroups. While it ensures representation, it lacks the statistical rigor of attribute sampling for formal audit conclusions.

References:

1. ISAC(2019). CISA Review Manual, 27th Edition. Chapter 1: The Process of Auditing Information Systems. The manual explicitly states, "Attribute sampling is the primary sampling method used for tests of controls... The purpose of attribute sampling is to estimate the rate of occurrence of a specific attribute or characteristic in a population." This directly aligns with testing the effectiveness of the physical access log system.

2. ISAC(n.d.). ISACA Glossary. "Attribute sampling—A sampling method used to estimate the proportion of a population that possesses a specified characteristic. This is the method used for compliance testing." This definition confirms its use for compliance testing.

3. Arens, A., Elder, R. J., & Beasley, M. S. (2016). Auditing and Assurance Services: An Integrated Approach. Pearson Education. Chapter 15 discusses audit sampling for tests of controls and substantive tests. It defines attribute sampling as the method auditors use to determine whether controls are operating effectively, focusing on the frequency of deviations from prescribed controls.

Question: 4

Which of the following is a corrective control?

A: Reviewing user access rights for segregation of duties

B: Executing emergency response plans

C: Verifying duplicate calculations in data processing

D: Separating equipment development, testing, and production

Correct Answer:

B

Explanation:

A corrective control is designed to correct and recover from errors or irregularities after they have been detected. Executing an emergency response plan is a quintessential corrective action. It is implemented after an incident has occurred with the express purpose of mitigating the impact, recovering systems, and restoring business operations to an acceptable state. The plan's execution directly addresses and corrects the problem (the emergency), which is the core function of a corrective control.

Why Incorrect Options are Wrong:

A: Reviewing user access rights for segregation of duties is a detective control. The review process is intended to identify violations or discrepancies, not to fix them.

C: Verifying duplicate calculations in data processing is a detective control. Its purpose is to find errors that have already occurred during processing, not to perform the correction itself.

D: Separating equipment development, testing, and production is a preventive control. It aims to stop unauthorized or flawed changes from being introduced into the live environment.

References:

1. ISACA CISA Review Manual, 27th Edition. Chapter 1, "The Governance and Management of IT," explicitly categorizes controls. It defines corrective controls as those that "are designed to correct errors or irregularities that have been detected." It lists "contingency planning" and "backup procedures" as examples, which are integral components of an emergency response plan. Conversely, it lists "reviews" and "reconciliations" as detective, and "segregation of duties" as preventive.

2. ISACA Glossary of Terms. The official ISACA glossary defines a Corrective Control as: "A control that is used to fix a problem, error, or irregularity." It defines a Detective Control as: "A control that is used to find a problem, error, or irregularity." This clearly distinguishes the function of option B (fixing) from options A and C (finding). (Source: ISACA Glossary, https://www.isaca.org/resources/glossary).

3. University Courseware. Information systems auditing courses consistently classify controls in this manner. For example, course materials often describe disaster recovery and emergency response as primary examples of corrective controls, while reconciliations and reviews are used as examples of detective controls. (e.g., materials based on the "Core Concepts of Information Systems Auditing" by The University of Texas at Dallas).

Question: 5

Which of the following should be an IS auditor's BEST recommendation to prevent installation of unlicensed software on employees' company-provided devices?

A: Enforce audit logging of software installation activities.

B: Remove unlicensed software from end-user devices.

C: Implement software blacklisting.

D: Restrict software installation authority to administrative users only.

Correct Answer:

D

Explanation:

The most effective and fundamental preventive control is to restrict the ability to perform the action in the first place. By limiting software installation authority to designated administrative users, an organization enforces the principle of least privilege. This control prevents standard users from installing any unauthorized software, licensed or not, thereby directly addressing the root cause of the risk. This is a broader and more proactive measure than other options.

Why Incorrect Options are Wrong:

A: Enforcing audit logging is a detective control. It records an installation after it has already occurred but does not prevent it.

B: Removing unlicensed software is a corrective control. It addresses the problem after the fact, rather than preventing the initial installation.

C: Software blacklisting is a preventive control, but it is less comprehensive than restricting installation rights. It only blocks known unwanted software and requires continuous updates to be effective.

References:

1. ISACA CISA Review Manual, 27th Edition. Chapter 4: Information Systems Operations. The manual emphasizes that a key control is to restrict access to system utilities and functions, such as software installation, based on the principle of least privilege. This ensures that only authorized personnel can make changes to systems.

2. ISACA, COBIT 2019 Framework: Governance and Management Objectives, 2018. The management objective APO07, Managed Human Resources, includes practices for defining roles and responsibilities, which involves granting appropriate levels of authority and privilege. Restricting installation rights is a direct application of this principle to manage operational risks. (Specifically, see practice APO07.03).

3. Kim, D., & Solomon, M. G. (2016). Fundamentals of Information Systems Security. Jones & Bartlett Learning. Chapter 5, "Access Control," describes how privilege management, including restricting administrative rights for standard users, is a foundational security control to prevent unauthorized system modifications, including software installation. This is a standard textbook used in university information security courses.

Question: 6

During a disaster recovery audit, an IS auditor finds that a business impact analysis (BIA) has not been performed The auditor should FIRST.

A: evaluate the impact on current disaster recovery capability.

B: issue an intermediate report to management

C: conduct additional compliance testing

D: perform business impact analysis

Correct Answer:

A

Explanation:

The Business Impact Analysis (BIA) is the foundational component for developing a disaster recovery plan (DRP). It identifies critical business processes and establishes key recovery metrics like Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Without a BIA, the existing DRP is based on assumptions rather than actual business requirements. Therefore, the auditor's immediate and primary task is to determine the significance of this deficiency by evaluating how the absence of a BIA affects the organization's ability to recover from a disaster. This evaluation quantifies the risk and is essential for formulating a meaningful audit finding and recommendation.

Why Incorrect Options are Wrong:

B: Issuing a report is a subsequent step. The auditor must first understand the full impact of the finding to provide a complete and accurate report to management.

C: Conducting additional compliance testing on a DRP that lacks a proper foundation (the BIA) would be inefficient and yield potentially misleading results about its true effectiveness.

D: The auditor's role is to provide independent assurance. Performing the BIA is a management responsibility; doing so would impair the auditor's independence and objectivity.

References:

1. ISACA, CISA Review Manual, 27th Edition. Chapter 4: Information Systems Operations and Business Resilience. The manual establishes that the BIA is the first and most critical step in the business continuity planning process. An auditor's role is to assess the adequacy

of this process. The absence of a BIA is a fundamental control weakness, and the auditor must assess its impact on the overall resilience strategy.

2. ISACA, CISA Glossary. "Business impact analysis (BIA): A process to determine the impact of losing the support of any resource to an enterprise... This information is used to make decisions about the management of business continuity." This definition underscores that without a BIA, decisions about recovery are uninformed. The auditor's first step is to assess the impact of these uninformed decisions. (URL: https://www.isaca.org/resources/glossary)

3. National Institute of Standards and Technology (NIST), Special Publication 800-34 Rev. 1, "Contingency Planning Guide for Federal Information Systems." Section 3.2, "Business Impact Analysis." This guide states, "The BIA is a key step in the contingency planning process... The BIA results are used to guide the remainder of the contingency planning process." This confirms the BIA's foundational role, and an auditor must first evaluate the consequences of its absence on the entire plan. (URL: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final, Page 15)

Question: 7

Which of the following BEST enables an IS auditor to detect incorrect exchange rates applied to outward remittance transactions at a financial institution?

A: Developing computer-assisted audit techniques (CAATs) during transaction audits

B: Performing sampling tests on transactions processed at the end of each day

C: Running continuous auditing scripts at the end of each day

D: Using supervised machine learning techniques to develop a regression model to predict incorrect input

Correct Answer:

A

Explanation:

Developing computer-assisted audit techniques (CAATs) is the most effective and comprehensive method for this task. CAATs enable an IS auditor to programmatically test 100% of the outward remittance transactions. The auditor can create a script or use specialized software to take the transaction data, independently look up the official exchange rate for the transaction date from a master file, recalculate the expected amount, and compare it to the amount recorded in the system. This approach directly identifies every single transaction with an incorrect rate, providing the highest level of assurance.

Why Incorrect Options are Wrong:

B: Sampling provides only reasonable, not absolute, assurance. It tests a small subset of transactions and could easily miss sporadic or systematic errors if they do not fall within the selected sample.

C: Continuous auditing is a methodology that uses CAATs. However, developing the CAAT (the tool/script) is the foundational enabling step. Option A is more precise as it names the specific technique required.

D: A regression model is a predictive, probabilistic tool. It is less precise for this task than a deterministic CAAT that compares data against a definitive source of truth (the official rate table).

References:

1. ISACA, CISA Review Manual, 27th Edition. Chapter 1, "The Process of Auditing Information Systems," details the use of CAATs for substantive testing. It states that CAATs are used to test details of transactions and balances, including performing recalculations to verify processing accuracy. This directly aligns with recalculating currency conversions to detect incorrect rates.

2. ISACA, (2014). CAATs and Other Electronic Audit Techniques. This white paper explains that a primary function of CAATs is to perform calculations and comparisons on entire populations of data, which is "more effective and efficient than testing a sample." (Page 5). This supports the superiority of CAATs over sampling for this scenario.

3. Gao, Y., & Yang, J. (2018). Application of Computer Assisted Audit Techniques. IEEE 3rd International Conference on Big Data Analysis (ICBDA). This paper discusses how CAATs are used for "detailed tests, such as recalculation... to check the accuracy of data processing." (Section III.A). This confirms that recalculation for accuracy checks is a core function of CAATs.

Question: 8

Which of the following is the BEST reason to utilize blockchain technology to record accounting transactions?

A: Integrity of records

B: Confidentiality of records

C: Availability of records

D: Distribution of records

Correct Answer:

A

Explanation:

The most significant benefit of using blockchain for accounting is the integrity of the records. Blockchain technology creates a distributed, immutable ledger where transactions are cryptographically linked in a chain. Each new block contains a hash of the previous block, making the ledger tamper-evident. Any attempt to alter a recorded transaction would require re-calculating all subsequent blocks, which is computationally infeasible and immediately detectable by all participants in the network. This inherent immutability provides a high degree of assurance regarding the integrity and auditability of financial records, which is a primary concern in accounting.

Why Incorrect Options are Wrong:

B: Confidentiality of records: This is incorrect because public blockchains are transparent by design, not confidential. While private or permissioned blockchains can incorporate privacy features, confidentiality is not a native or primary benefit of the core technology.

C: Availability of records: While the distributed nature of blockchain enhances availability, this is a secondary benefit. High availability can also be achieved with traditional replicated database systems. The unique value proposition for accounting is immutability, not just availability.

D: Distribution of records: Distribution is a feature or the mechanism of blockchain, not the ultimate benefit itself. The distribution of the ledger is what enables the primary benefits of integrity (through consensus) and availability.

References:

1. ISACA, Blockchain and Internal Control: The COSO Perspective, 2019. This white paper states, "The key features of blockchain that are relevant from a business and internal control perspective are... Immutability and data integrity... Once a transaction is added to the blockchain, it is permanent and cannot be altered." This directly supports integrity as a key reason.

2. Dai, J., & Vasarhelyi, M. (2017). "Toward Blockchain-Based Accounting and Assurance." Journal of Information Systems, 31(3), 5–21. (Published by the American Accounting Association). The paper highlights, "The append-only and immutable data structure of the blockchain makes it a good technology for accounting... transactions recorded on the blockchain are immutable, preventing them from being altered or deleted." (p. 8). This emphasizes immutability as the core benefit for accounting.

3. Yermack, (2017). "Corporate Governance and Blockchains." Review of Finance, 21(1), 7–31. (Oxford University Press). This academic review notes that a key advantage of blockchain is that "records on the blockchain are immutable... This feature offers the potential for major improvements in accounting and auditing." (p. 10).

Question: 9

Which ofthe following is the BEST way for an IS auditorto reduce sampling risk when performing audit sampling to verify the adequacy of an organization's internal controls?

A: Lower the sample standard deviation

B: Decrease the sampling size

C: Outsource the sampling process.

D: Use a statistical sampling method

Correct Answer:

D

Explanation:

Statistical sampling is the BEST way to reduce sampling risk because it applies the laws of probability to select and evaluate a sample. This allows an IS auditor to quantitatively measure and control sampling risk to a specified level. By using statistical methods, the auditor can objectively determine an appropriate sample size, select a representative sample, and project the results to the entire population with a known confidence level and precision, thereby minimizing the risk of drawing an incorrect conclusion from the sample.

Why Incorrect Options are Wrong:

A: Lower the sample standard deviation: An auditor cannot directly lower the standard deviation; it is an inherent measure of variability within the population. It is a factor used to calculate sample size, not an action to reduce risk.

B: Decrease the sampling size: Decreasing the sample size increases sampling risk. A smaller sample is less likely to be representative of the population, raising the probability of an incorrect conclusion.

C: Outsource the sampling process: Outsourcing is a resourcing decision. It does not inherently change the statistical properties or risks of the sampling methodology itself. The risk remains regardless of who performs the task.

References:

1. ISAC(2019). CISA Review Manual, 27th Edition. Chapter 1, The Process of Auditing Information Systems. The manual states, "The main advantage of statistical sampling is that it allows the IS auditor to quantify, measure and control sampling risk." It also explains that

population variability (standard deviation) is a key factor in determining sample size, not something the auditor actively lowers.

2. ISAC(2014). ISACA G20: Audit Sampling. Page 10. This guideline explicitly states, "Statistical sampling allows the IS auditor to...control the risk of drawing an incorrect conclusion from the sample (sampling risk)." It contrasts this with nonstatistical sampling, where sampling risk cannot be quantitatively measured.

3. Arens, A., Elder, R. J., & Beasley, M. S. (2016). Auditing and Assurance Services: An Integrated Approach. Pearson. Chapter 15, "Audit Sampling for Tests of Controls and Substantive Tests of Transactions." This academic text details that using statistical methods is the primary way auditors manage and quantify sampling risk, distinguishing it from nonstatistical methods where risk assessment is purely judgmental.

Question: 10

Which of the following provides the MOST assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system?

A: Comparing code between old and new systems

B: Loading balance and transaction data to the new system

C: Running historical transactions through the new system

D: Reviewing quality assurance (QA) procedures

Correct Answer:

C

Explanation:

Running historical transactions through the new system and comparing the output with the results from the old system is a form of parallel simulation. This is a powerful substantive testing technique that provides the highest level of assurance regarding processing integrity. It directly validates the new system's logic for completeness and accuracy using a known set of inputs and expected outcomes. This method effectively tests the end-to-end processing functionality against a verified baseline, which is the core concern of the question.

Why Incorrect Options are Wrong:

A: Comparing code is a static analysis technique that is often impractical and does not confirm the accuracy of processing outcomes with real data.

B: Loading balance and transaction data primarily tests the accuracy of data migration, not the system's ongoing transaction processing logic.

D: Reviewing quality assurance (QA) procedures assesses the testing process itself, providing only indirect assurance about the system's actual performance and accuracy.

References:

1. ISACA CISA Review Manual, 27th Edition. Domain 3: Information Systems Acquisition, Development, and Implementation. The manual describes various testing methods, including parallel testing, where a new system is run alongside the old one. Reprocessing historical transactions is a form of this, providing direct evidence by comparing the new system's output to a known, correct baseline, thus offering high assurance.

2. Weber, R. (1999). Information Systems Control and Audit. Prentice Hall. Chapter 15, "Auditing Computer Applications I," discusses parallel simulation as a key technique for auditors to verify application processing. It states, "Parallel simulation involves processing production data using a computer program that simulates the logic of the application program being reviewed... The major advantage of parallel simulation is that it allows the auditor to test the application with a large volume of live data." (p. 558). This directly supports using historical transactions for assurance.

3. Hall, J. (2018). Information Technology Auditing, 4th Edition. Cengage Learning. Chapter 4, "Auditing the IT Governance Process," details substantive tests, including parallel simulation, as a method to "reprocess data from a previous period and compare the results with the original output." This is presented as a technique to gain assurance over application logic.

Question: 11

An IS auditor begins an assignment and identifies audit components for which the auditoris not qualified to assess. Which of the following is the BEST course of anion?

A: Exclude the related tests from the audit plan and continue the assignment.

B: Notify audit management for a decision on how to proceed

C: Complete the audit and give full disclosure in the final audit report

D: Complete the work assignment to the best of the auditor's Ability

Correct Answer:

B

Explanation:

According to the ISACA Code of Professional Ethics, IS auditors must maintain competency and only undertake activities they can reasonably expect to complete with the necessary skills and knowledge. When an auditor identifies a personal competency gap, the most appropriate and professional action is to escalate the issue to audit management. This allows management to make an informed decision, such as assigning a specialist, providing additional resources, or formally modifying the audit scope in consultation with stakeholders. This course of action upholds the principles of due professional care and ensures the integrity and quality of the audit engagement.

Why Incorrect Options are Wrong:

A: Unilaterally excluding tests from the audit plan is inappropriate. It compromises the audit's intended scope and fails to address identified risks without proper authorization from audit management.

C: Completing the audit and disclosing the lack of competence in the report is a violation of professional standards. The primary duty is to perform the audit competently, not to report on one's own incompetence after the fact.

D: Proceeding with a "best effort" approach is unacceptable when the auditor's ability is below the required professional standard. This violates the core ethical requirement to be competent for the assigned work.

References:

1. ISACA, ITAF: A Professional Practices Framework for IS Audit/Assurance, 4th Edition, (2020). Standard 1202 Competence states, "The IS audit and assurance function should be collectively competent, having the skills and knowledge to perform the planned audit and assurance work." Guideline 2203, related to staffing, notes that management is responsible for ensuring the team has the required skills. Escalation is the necessary step to enable this.

2. ISACA, Code of Professional Ethics. The code explicitly requires members to: "Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence." Notifying management is the direct application of this principle when a gap is found. (Available at: https://www.isaca.org/credentialing/code-of-professional-ethics)

3. ISACA, CISA Review Manual, 27th Edition. Chapter 1, "The Process of Auditing Information Systems," emphasizes that if the audit team lacks the required technical skills, it should obtain assistance from experts. The individual auditor's responsibility is to report this need to management.

Question: 12

During business process reengineering (BPR) of a bank's teller activities, an IS auditor should evaluate:

A: the impact of changed business processes.

B: the cost of new controls.

C: BPR project plans

D: continuous improvement and monitoring plans.

Correct Answer:

A

Explanation:

The primary role of an IS auditor during a Business Process Reengineering (BPR) initiative is to provide assurance that the redesigned processes align with business objectives and incorporate adequate internal controls. Evaluating the impact of the changed processes is the most comprehensive activity, as it includes assessing new risks, the effectiveness of new controls, and the overall effect on the control environment. This evaluation ensures that the reengineering effort does not inadvertently introduce vulnerabilities or weaken the organization's governance and control framework.

Why Incorrect Options are Wrong:

B: The cost of new controls is a management consideration; the auditor's primary focus is on control adequacy and effectiveness, not just the cost.

C: Reviewing project plans is an initial step to understand scope, but evaluating the actual impact of the changes is the core audit activity during the project.

D: Continuous monitoring plans are evaluated to ensure long-term effectiveness, which is typically a post-implementation concern, not the primary focus during BPR.

References:

1. ISACA CISA Review Manual, 27th Edition. Chapter 2: Governance and Management of IT. The manual emphasizes the IS auditor's role in reviewing significant changes to business processes to ensure that controls are considered, designed, and implemented effectively. This directly relates to assessing the impact of the BPR.

2. ISACA, "Business Process Reengineering," Audit Program, 2018. This official ISACA audit program outlines key steps for auditing BPR, including "Evaluate the impact of the BPR project on the existing IT environment and internal controls" and "Determine whether key controls have been identified and incorporated into the reengineered business process." (Available via ISACA membership portal).

3. Hammer, M., & Champy, J. (1993). Reengineering the Corporation: A Manifesto for Business Revolution. HarperBusiness. This foundational text on BPR highlights that reengineering involves radical redesign, which inherently carries new risks and impacts that must be managed. An auditor's role is to provide assurance over this management of impact. (Section: "The New World of Work").

Question: 13

When reviewing a project to replace multiple manual data entry systems with an artificial intelligence (AI) system, the IS auditor should be MOST concerned with the impact At will have on:

A: task capacity output

B: employee retention

C: future task updates

D: enterprise architecture (EA).

Correct Answer:

D

Explanation:

The replacement of multiple manual systems with a single, transformative technology like Artificial Intelligence (AI) constitutes a fundamental change to the organization's IT landscape. The IS auditor's most significant concern is the impact on the Enterprise Architecture (EA). The EA provides the holistic blueprint for aligning business processes, data, applications, and technology infrastructure with strategic objectives. Ensuring the new AI system integrates properly within the EA is critical for maintaining data integrity, security, interoperability, and overall IT governance. A failure at the architectural level poses the most systemic and far-reaching risk to the enterprise.

Why Incorrect Options are Wrong:

A: task capacity output: This is an important operational performance metric, but it is a component concern that is addressed within the broader business case and architectural planning, not the primary strategic risk.

B: employee retention: This is a significant human resources and change management issue. While relevant to the project's overall success, it is a secondary effect from the IS auditor's primary focus on information systems, controls, and governance.

C: future task updates: This is a valid system lifecycle and maintenance concern. However, the strategy for updates and maintenance is a detail that should be defined and governed by the overarching enterprise architecture.

References:

1. ISACA, CISA Review Manual, 27th Edition, Chapter 2: Governance and Management of IT. This chapter emphasizes that Enterprise Architecture provides the fundamental "organizing logic for business processes and IT infrastructure," reflecting the integration of business, information, applications, and technology. A project of this magnitude directly impacts this core structure, making it a primary audit concern.

2. ISACA, COBIT 2019 Framework: Governance and Management Objectives, APO03 Manage Enterprise Architecture. The purpose of this process is to "represent the different building blocks that make up the enterprise and their interrelationships... to enable and support the achievement of business objectives." The introduction of a central AI system fundamentally alters these building blocks and their relationships, requiring stringent architectural review.

3. Janssen, M., & van der Voort, H. (2020). "The role of enterprise architecture in transforming the public sector." Government Information Quarterly, 37(3). While focused on the public sector, this peer-reviewed article highlights that EA is essential for managing complex transformations driven by new technologies like AI, ensuring alignment and mitigating systemic risks. The principles are directly applicable to any enterprise.

Question: 14

Which of the following weaknesses would have the GREATEST impact on the effective operation of a perimeter firewall?

A: Potential back doors to the firewall software

B: Use of stateful firewalls with default configuration

C: Ad hoc monitoring of firewall activity

D: Misconfiguration of the firewall rules

Correct Answer:

D

Explanation:

A perimeter firewall's effectiveness is fundamentally determined by its rule set, which implements the organization's security policy. A misconfiguration of these rules directly undermines the firewall's primary purpose of filtering traffic correctly. A single incorrect rule can create a significant vulnerability, allowing malicious traffic in or blocking legitimate business-critical traffic, thereby having the greatest and most immediate impact on the firewall's effective operation. The firewall may be technically functional, but it is failing to perform its intended security function.

Why Incorrect Options are Wrong:

A: Potential back doors to the firewall software: While a backdoor is a critical vulnerability, it is a potential weakness that may or may not be exploited. A misconfiguration is an active and certain failure in the firewall's operational logic.

B: Use of stateful firewalls with default configuration: This is a specific example of a misconfiguration. Option D is broader and more encompassing, as misconfigurations can also include incorrect rule ordering or overly permissive custom rules, not just defaults.

C: Ad hoc monitoring of firewall activity: This is a weakness in a detective control process (monitoring), not in the firewall's primary preventive operation. A correctly configured firewall is still operating effectively even if it is poorly monitored.

References:

1. ISACA, CISA Review Manual, 27th Edition. Chapter 4, Information Systems Operations—Network Infrastructure Security. The manual emphasizes that a key audit step for firewalls is

to "review the firewall rule set to ensure it is aligned with policy requirements." This highlights that the rule set's configuration is the paramount factor in its effectiveness. Misconfiguration represents a direct failure to meet these requirements.

2. National Institute of Standards and Technology (NIST), Special Publication 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy. Section 4.3, "Firewall Security Issues," states: "The most common firewall security issues are related to firewall policies and rule sets that are not configured correctly... A single error in a rule set can allow unauthorized access that completely negates the firewall's value." (p. 23). This directly supports that misconfiguration has the greatest impact.

3. Wool, (2004). "A quantitative study of firewall configuration errors." IEEE Computer, 37(6), 62-67. This academic study analyzes real-world firewall configurations and concludes that "configuration errors are rampant" and are a primary source of network security vulnerabilities, reinforcing that misconfiguration is a critical and impactful weakness.

Question: 15

The PRIMARY benefit of information asset classification is that it:

A: facilitates budgeting accuracy.

B: enables risk management decisions.

C: prevents loss of assets.

D: helps to align organizational objectives.

Correct Answer:

B

Explanation:

The primary benefit of information asset classification is to provide a basis for risk management. By categorizing assets according to their value, sensitivity, and criticality, an organization can make informed decisions about the appropriate level of security controls required to protect them. This process is foundational to risk assessment, as it helps determine the potential business impact if an asset's confidentiality, integrity, or availability is compromised. Consequently, classification directly enables risk-based decisions on security investments and control implementation.

Why Incorrect Options are Wrong:

A: Budgeting is a secondary benefit. While classification informs the selection of controls, which have budget implications, its primary purpose is risk-based decision-making, not just financial planning.

C: Classification itself does not prevent loss; it is a prerequisite. The security controls implemented based on the classification are what prevent loss.

D: This is too broad. While the overall security program aligns with organizational objectives, the specific, primary function of asset classification is to facilitate risk management, not strategic alignment directly.

References:

1. ISACA CISA Review Manual, 27th Edition. Domain 3: Information Systems Acquisition, Development, and Implementation. The manual emphasizes that data classification is a key control for determining the value of data and is a prerequisite for applying appropriate security measures based on risk. It directly links classification to risk management by

stating its purpose is to ensure that information assets receive a level of protection appropriate to their risk level.

2. ISACA, "Information Asset Classification and Handling," (2020). This official ISACA white paper states, "The primary purpose of information classification is to enable the organization to make risk-based decisions on how to protect its information assets." (Page 4). It explicitly connects the act of classification to the process of risk management.

3. University of Washington, "Information Security and Risk Management Standard." This university standard outlines that "Information classification is a key component of the UW's risk management strategy." It details how classification levels (Confidential, Restricted, Public) directly determine the security controls required, which is a core risk management activity. Available at: https://itconnect.uw.edu/work/wp-content/uploads/2018/03/Information-Security-and-Risk-Management-Standard.pdf (Section 2.1).

Question: 16

Which of the following is the GREATEST threat to Voice-over Internet Protocol (VoIP) related to privacy?

A: Call recording

B: Incorrect routing

C: Eavesdropping

D: Denial of service (DoS)

Correct Answer:

C

Explanation:

Eavesdropping is the unauthorized real-time interception of private communications, such as a phone call. In a Voice-over Internet Protocol (VoIP) environment, voice is converted into data packets and sent over an IP network. This makes VoIP traffic susceptible to the same packet-sniffing tools used to intercept other data. An attacker can capture these packets and reconstruct the conversation, directly violating the privacy and confidentiality of the communicating parties. Among the choices, eavesdropping represents the most direct and fundamental threat to the privacy of the call's content.

Why Incorrect Options are Wrong:

A: Call recording is a method of capturing a conversation, but eavesdropping is the broader, fundamental act of unauthorized listening that directly violates privacy. Recording is a result of a successful eavesdropping attack.

B: Incorrect routing is primarily a threat to service availability and integrity. While it could inadvertently expose a call to an unauthorized party, its main impact is preventing the call from connecting correctly.

D: Denial of service (DoS) is an attack on availability. It aims to make the VoIP service unusable by overwhelming it with traffic, thus preventing calls, but it does not compromise the privacy of call content.

References:

1. ISACA CISA Review Manual, 27th Edition. Chapter 4: Information Systems Operations. The manual discusses that data transmitted over networks, including VoIP, is subject to interception (eavesdropping), which is a primary threat to confidentiality and privacy.

2. Sidor, (2013). VoIP Security. ISACA Journal, vol. 2. This article identifies eavesdropping as a key security risk for VoIP, stating, "Eavesdropping on calls is a major concern... Without encryption, VoIP conversations are sent in the clear, making them easy to intercept." (Direct URL: https://www.isaca.org/resources/isaca-journal/past-issues/2013/voip-security)

3. Singh, S., & Agrawal, (2012). VoIP Security Challenges: A Survey. I.J. Modern Education and Computer Science, 4(2), 44-53. In their survey of VoIP threats, the authors categorize eavesdropping as a primary attack against confidentiality (privacy), noting its ease of execution on unsecured networks. (Direct URL: https://mecs-press.org/ijmecs/ijmecs-v4-n2/IJMECS-V4-N2-6.pdf, Section 3.1)

Question: 17

Which of the following should be a concern to an IS auditor reviewing a digital forensic process for a security incident?

A: The media with the original evidence was notwrite-btocked.

B: The forensic expert used open-source forensic tools.

C: The affected computer was not immediately shut down after theincident.

D: Analysis was performed using an image of the original media.

Correct Answer:

A

Explanation:

The primary objective in digital forensics is to preserve the integrity of the original evidence. Failing to use a write-blocker on the source media is a critical procedural failure. A write-blocker is a hardware or software tool that prevents any write operations to the storage device, ensuring that the original evidence is not altered during the acquisition (imaging) process. Without this protection, data on the original media could be modified, which would compromise the forensic soundness of the evidence and its admissibility in legal or disciplinary proceedings. This represents the most significant concern for an IS auditor reviewing the process.

Why Incorrect Options are Wrong:

B: The use of validated and widely accepted open-source forensic tools is a common practice and not inherently a concern. The tool's reliability matters, not its licensing model.

C: Not immediately shutting down a system is often a deliberate and correct action to preserve volatile data (e.g., RAM contents, network connections) which would be lost.

D: Performing analysis on a forensic image (a bit-for-bit copy) rather than the original media is the standard and required best practice to protect the original evidence.

References:

1. ISACA, CISA Review Manual, 27th Edition. Domain 5: Protection of Information Assets. The manual emphasizes that a key control in forensic evidence collection is ensuring the original media is protected from alteration, typically through the use of write-blockers, and that analysis is performed on a copy.

2. National Institute of Standards and Technology (NIST) Special Publication 800-86, "Guide to Integrating Forensic Techniques into Incident Response," Section 3.3.1, Acquiring the Data. This guide states, "When acquiring data from a disk, a hardware write blocker should be used to ensure that the original disk is not modified." (Page 19).

3. Carrier, B., "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers," International Journal of Digital Evidence, Fall 2002, Volume 1, Issue 4. This foundational academic paper discusses the forensic process, highlighting the necessity of preventing modification to the original evidence source as a core principle. The use of write-blockers is a direct implementation of this principle. (Available through various academic databases).

Question: 18

What is the BEST control to address SQL injection vulnerabilities?

A: Input validation

B: Unicode translation

C: Secure Sockets Layer (SSL) encryption

D: Digital signatures

Correct Answer:

A

Explanation:

Input validation is the most effective and direct control to prevent SQL injection (SQLi) vulnerabilities. This process involves checking and sanitizing all data received from a user or external source to ensure it conforms to expected formats and does not contain malicious SQL commands. By validating input on the server side before it is incorporated into a database query, the application can reject or neutralize the malicious code, thus preventing the attack from ever reaching the database for execution.

Why Incorrect Options are Wrong:

B: Unicode translation: This is a character encoding process. While improper handling can be exploited to bypass weak filters, it is not the primary control against SQL injection itself.

C: Secure Sockets Layer (SSL) encryption: SSL/TLS encrypts data in transit, protecting it from eavesdropping. It does not inspect or validate the data's content, so malicious SQL commands are simply passed through the encrypted channel.

D: Digital signatures: These provide message integrity and sender authentication. They do not prevent a legitimate (but malicious) user from submitting harmful input to an application.

References:

1. ISACA CISA Review Manual, 27th Edition. Chapter 5: Protection of Information Assets. This manual extensively covers application controls, identifying input validation as a fundamental control for ensuring data integrity and preventing injection-style attacks like SQLi. It emphasizes that all user input should be validated for type, length, and format.

2. MIT OpenCourseWare (OCW), 6.858 Computer Systems Security, Fall 2014. Lecture 16: Web Security. The course materials explicitly identify input validation and the use of prepared statements (parameterized queries) as the two primary defenses against SQL injection attacks. (URL: https://ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/resources/lec16/)

3. Kaur, K., & Singh, (2015). A Survey of SQL Injection Attacks, Techniques and Prevention. IEEE International Conference on Computing, Communication & Automation. This peer-reviewed paper categorizes countermeasures for SQLi, placing input validation and sanitization in the primary "Server-Side Scripts" defense category as a critical preventative measure. (DOI: 10.1109/CCAA.2015.7148429)

Question: 19

When engaging services from external auditors, which of the following should be established FIRST?

A: Termination conditions agreements

B: Nondisclosure agreements

C: Service level agreements

D: Operational level agreements

Correct Answer:

B

Explanation:

When engaging any external party, including auditors, who will be granted access to sensitive or confidential information, a nondisclosure agreement (NDA) must be the first legal instrument established. The NDA provides a legal framework for protecting the organization's proprietary data before any substantive discussions about the scope of work, service levels, or contract terms can occur. These subsequent negotiations require the sharing of information that would be at risk without a pre-existing confidentiality agreement. Establishing the NDA first is a foundational step in third-party risk management.

Why Incorrect Options are Wrong:

A: Termination conditions agreements: These are critical components of the main service contract but are negotiated and finalized after initial confidential discussions, which are protected by the NDA.

C: Service level agreements (SLAs): Defining an SLA requires a detailed understanding of the systems and processes to be audited. This information is confidential and should only be shared after an NDA is signed.

D: Operational level agreements (OLAs): OLAs are internal agreements between an organization's own departments to support an SLThey are not established with external parties like auditors.

References:

1. ISACA CISA Review Manual, 27th Edition. Chapter 1, Section 1.4.4, "Sourcing Practices," emphasizes the need for contracts with third parties to include provisions for

confidentiality. The logical and prudent sequence for risk management is to secure confidentiality via an NDA before sharing the information needed to draft the full contract.

2. ISACA, Vendor Management Using COBIT 5, 2014. The vendor management life cycle begins with identifying needs and selecting vendors. This phase involves due diligence, which necessitates the sharing of sensitive information. An NDA is a prerequisite for this information exchange to occur securely. (See Figure 2—Vendor Management Life Cycle).

3. Brotby, W. K., Information Security Governance: A Practical Development and Implementation Approach, ISACA, 2009. Chapter 6, "Third-Party Governance," outlines that legal agreements, including NDAs, are essential early in the relationship to protect the organization during due diligence and subsequent service delivery. This establishes the priority of confidentiality.

Question: 20

Which of the following is the BEST indicator of the effectiveness of signature-based intrusion detection systems (IDSs)?

A: An increase in the number of internally reported criticalincidents

B: An increase in the number of detected incidents not previously identified

C: An increase in the number of identified false positives

D: An increase in the number of unfamiliar sources ofintruders

Correct Answer:

B

Explanation:

The effectiveness of a signature-based Intrusion Detection System (IDS) is best measured by its ability to accurately detect malicious activities based on its known signature database. An increase in the number of detected incidents that were not previously identified indicates that the IDS is now successfully identifying threats that it previously missed (i.e., reducing its false negative rate). This improvement is a direct indicator of enhanced effectiveness, often resulting from updated signatures that can recognize new or variant attack patterns.

Why Incorrect Options are Wrong:

A: An increase in internally reported critical incidents suggests the IDS is failing to detect them, indicating a high rate of false negatives and thus, ineffectiveness.

C: An increase in false positives means the IDS is incorrectly flagging benign traffic as malicious. This indicates poor tuning and reduced, not enhanced, effectiveness.

D: The source of intruders is an external factor. While the IDS reports this information, a change in source does not inherently measure the IDS's performance or accuracy in detecting attacks.

References:

1. National Institute of Standards and Technology (NIST) Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS). Section 5.3, "IDPS Maintenance," discusses the importance of signature updates. It states, "New attacks and new variants of existing attacks are constantly being developed, so signatures must be updated to detect them." Detecting incidents not previously identified (Option B) is a direct result of this

effective maintenance. Section 5.2 also notes that false negatives are a primary security problem, so reducing them is a key goal. (Direct URL: https://csrc.nist.gov/publications/detail/sp/800-94/final)

2. ISACA, CISA Review Manual, 27th Edition. Domain 4: Information Systems Operations and Business Resilience. The manual emphasizes that a primary goal of an IDS is to detect attacks. Its effectiveness is tied to the quality and currency of its signature files. An increase in detected incidents that were previously missed demonstrates that the system's detection capabilities have improved, fulfilling its core purpose.

3. Kaur, J., & Singh, (2013). A Survey of Intrusion Detection Systems. International Journal of Computer Science and Information Technologies, 4(3), 453-456. This academic review notes that a key performance metric for an IDS is its detection rate (the ratio of detected intrusions to the total number of intrusions). An increase in detected incidents (Option B) directly corresponds to an improved detection rate.

Question: 21

Which of the following is the MOST important step in the development of an effective IT governance action plan?

A: Setting up an IT governance framework for the process

B: Conducting a business impact analysis (BIA)

C: Measuring IT governance key performance indicators (KPIs)

D: Preparing a statement of sensitivity

Correct Answer:

A

Explanation:

An effective IT governance action plan must be aligned with the organization's strategic objectives. The most important step in its development is establishing an IT governance framework (e.g., COBIT). This framework provides the necessary structure, principles, processes, and organizational structures. It defines the "what" and "why" of governance, creating the foundation upon which a detailed action plan (the "how" and "when") can be built. Without a guiding framework, any action plan would be ad-hoc, lack strategic alignment, and be difficult to measure, rendering it ineffective.

Why Incorrect Options are Wrong:

B: Conducting a business impact analysis (BIA): A BIA is a critical input for business continuity and risk management components within the governance framework, but it does not establish the overall governance structure itself.

C: Measuring IT governance key performance indicators (KPIs): Measuring KPIs is a control and monitoring activity performed after an action plan is implemented to assess its effectiveness, not a foundational step in its development.

D: Preparing a statement of sensitivity: This is a specific task related to data classification within information security management, a subset of IT governance, not the primary step for the entire governance plan.

References:

1. ISACA, COBIT® 2019 Framework: Introduction and Methodology, 2018, Page 31. The COBIT framework is described as the foundation for an enterprise's governance system for

information and technology (I&T). The implementation guide shows that defining the framework and its components precedes the creation of detailed improvement plans.

2. ISACA, COBIT® 2019 Implementation Guide, 2018, Pages 15-25. The implementation life cycle's initial phases ("What are the drivers?", "Where are we now?", "Where do we want to be?") are dedicated to establishing the scope, goals, and structure of the governance system (the framework) before developing the action plan in Phase 4 ("What needs to be done?").

3. De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5. Springer International Publishing, Page 97. The authors describe the implementation of IT governance as a process that begins with creating the right environment and structure (the framework), from which specific improvement projects (action plans) are derived.

Question: 22

Which of the following is a benefit of the DevOps development methodology?

A: It leads to a well-defined system development life cycle (SDLC)

B: It enforces segregation of duties between code developers and release migrators.

C: It enables increased frequency of software releases to production.

D: It restricts software releases to a fixed release schedule

Correct Answer:

C

Explanation:

The primary goal and most significant benefit of the DevOps methodology is to shorten the systems development life cycle and provide continuous delivery with high software quality. This is achieved by integrating development (Dev) and operations (Ops) teams and automating the software delivery pipeline (CI/CD). This integration and automation directly enable a higher frequency of software releases to production, allowing organizations to deliver value to customers more rapidly and respond to market changes more effectively.

Why Incorrect Options are Wrong:

A: While DevOps is a methodology, it is characterized by flexibility and continuous flow, not a rigid, "well-defined" sequential structure like the traditional Waterfall model. Its definition lies in its principles and practices, not in fixed phases.

B: This is contrary to the DevOps philosophy. DevOps aims to break down silos and reduce the strict segregation of duties between developers and operations teams, fostering a culture of shared responsibility.

D: This describes a traditional release model (e.g., Waterfall). DevOps specifically moves away from fixed, infrequent release schedules to enable on-demand or much more frequent, smaller releases.

References:

1. ISACA, CISA Review Manual, 27th Edition, 2019. Chapter 3, Section: "Systems Development Methodologies." The manual describes DevOps as a practice that "emphasizes the collaboration and communication of both software developers and other information technology (IT) professionals while automating the process of software delivery

and infrastructure changes. It aims to establish a culture and environment where building, testing and releasing software can happen rapidly, frequently and more reliably." This directly supports the increased frequency of releases.

2. Lwakatare, L. E., et al. (2019). "DevOps in practice: A multiple case study of five companies." Information and Software Technology, vol. 114, pp. 217-230. This study identifies key benefits of DevOps, stating, "The most frequently reported benefit was improved deployment frequency and reduced lead time for changes." (Section 4.1).

3. Ebert, C., Gallardo, G., Hernantes, J., & Serrano, N. (2016). "DevOps." IEEE Software, 33(3), 94-100. This article states, "DevOps aims to deliver software and services at high velocity... Key practices include continuous integration and continuous delivery (CI/CD), which enable frequent releases." (p. 94).

Question: 23

When evaluating a protect immediately prior to implementation, which of the following would provide the BEST evidence that the system has the required functionality?

A: User acceptance testing (UAT) results

B: Quality assurance (QA) results

C: Integration testing results

D: Sign-off from senior management

Correct Answer:

A

Explanation:

User acceptance testing (UAT) is the final phase of testing before a system is implemented. Its primary purpose is for end-users to validate that the system meets their specific business requirements and can perform the functions for which it was designed. Therefore, successful UAT results provide the most direct and best evidence that the system has the required functionality from a business perspective, confirming it is fit for purpose immediately prior to going live.

Why Incorrect Options are Wrong:

B: Quality assurance (QA) results: QA is a broad set of activities focused on ensuring quality throughout the entire development process, not a specific test phase. "QA results" is too general compared to the specific evidence provided by UAT.

C: Integration testing results: Integration testing verifies that different system modules and components work together correctly. It does not, however, confirm that the system as a whole meets the end-user's business requirements.

D: Sign-off from senior management: This is a formal approval or authorization to proceed, which is typically based on the evidence from UAT. The sign-off itself is not the primary evidence of functionality.

References:

1. ISACA CISA Review Manual, 27th Edition, Chapter 3: Information Systems Acquisition, Development and Implementation. This manual describes User Acceptance Testing (UAT)

as the process where users test the system to ensure it meets their business needs. It is positioned as a critical final check on functionality before implementation.

2. ISACA Glossary of Terms. Defines User Acceptance Testing (UAT) as: "A process to obtain confirmation by a user that a system meets mutually agreed-upon requirements." This definition directly links UAT to confirming "required functionality." (Source: ISACA official website glossary).

3. Sommerville, I. (2016). Software Engineering (10th ed.). Pearson. In academic software engineering literature, UAT is consistently presented as the stage where the client or end-user validates the software against their original requirements before accepting the final product for deployment (Chapter 8: Software Testing).

Question: 24

An IS auditor finds that the process for removing access for terminated employee is not documented. What is the MOST significant risk from this observation?

A: Access rights may not be removed in a timely manner

B: Unauthorized access cannot be identified

C: Procedures may not align with the practices

D: HR records may not match systemaccess

Correct Answer:

A

Explanation:

The absence of a documented process for removing access upon employee termination creates a significant risk of inconsistency and oversight. The most direct and severe consequence is that access rights are not revoked promptly or are missed altogether. This failure in the de-provisioning process leaves a critical window of vulnerability where a former employee can retain access to sensitive systems and data. Timely revocation of access is a fundamental control in identity and access management (IAM) designed to prevent unauthorized activities by individuals who are no longer authorized.

Why Incorrect Options are Wrong:

B: Unauthorized access cannot be identified: The primary risk is the failure to prevent unauthorized access by revoking credentials, not the failure to detect it later. Detection is a separate control (e.g., log review).

C: Procedures may not align with the practices: This statement describes the current state (no documented procedure exists) rather than the resulting risk. The risk is the negative consequence of this state.

D: HR records may not match system access: This mismatch is an indicator of the control failure. The actual risk is the retained access that this mismatch represents, not the discrepancy itself.

References:

1. ISACA, CISA Review Manual, 27th Edition. Domain 4: Information Systems Operations, Section 4.4 User Access. The manual emphasizes that formal, documented procedures are

essential for managing the entire user access lifecycle. It explicitly states that upon termination, access rights must be removed in a timely manner to mitigate the risk of unauthorized access by former employees. The lack of a process directly undermines this core control objective.

2. National Institute of Standards and Technology (NIST), Special Publication 800-53, Revision 5. Security and Privacy Controls for Information Systems and Organizations, Control Family: Access Control (AC), Control: AC-2 Account Management. This standard mandates that organizations must "disable information system accounts automatically after a defined period of inactivity" and "disable/remove accounts for terminated or transferred users in a timely manner." The absence of a documented process directly leads to the risk of non-compliance and untimely removal. (URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final, Page: AC-3)

3. Kim, D., & Solomon, M. G. (2016). Fundamentals of Information Systems Security. Jones & Bartlett Learning. Chapter 5, "Identity and Access Management," discusses the principle of least privilege and the importance of the user access lifecycle. It highlights that the termination phase (de-provisioning) is critical and delays create direct security risks. A documented, repeatable process is presented as the primary mechanism to ensure timeliness.

Question: 25

An organization is running servers with critical business application that are in an area subject to frequent but brief power outages. Knowledge of which of the following would allow the organization's management to monitor the ongoing adequacy of the uninterruptable power supply (UPS)?

A: Number of servers supported by the ups

B: Duration and interval of the power outages

C: Business impact of server downtime

D: Mean time to recover servers afterfailure

Correct Answer:

B

Explanation:

To monitor the ongoing adequacy of an uninterruptible power supply (UPS), management must compare its performance capability against the specific threat it mitigates. In this scenario, the threat is "frequent but brief power outages." The primary performance characteristic of a UPS relevant to this threat is its runtime (how long it can supply power). By monitoring the actual duration and interval of the power outages, management can continuously assess whether the UPS's runtime is sufficient. If outage durations begin to exceed the UPS's designed runtime, the control is no longer adequate.

Why Incorrect Options are Wrong:

A: Number of servers supported by the ups: This relates to the initial load capacity sizing of the UPS, not the ongoing monitoring of its adequacy against outage duration.

C: Business impact of server downtime: This is used in a Business Impact Analysis (BIA) to justify the need for a UPS and set recovery objectives, not to monitor its technical performance.

D: Mean time to recover servers after failure: This is a reactive metric for incident response effectiveness after a failure has already occurred. A UPS is a preventative control designed to avoid failure.

References:

1. ISACA, CISA Review Manual, 27th Edition. Domain 4: Information Systems Operations, Section 4.4, "Information Systems Operations." The manual emphasizes that the selection and maintenance of environmental controls like a UPS must be based on a risk assessment. Monitoring the characteristics of the threat (power outages) is essential to ensure the control remains effective in mitigating that specific risk.

2. IEEE Std 1100-2005, "IEEE Recommended Practice for Powering and Grounding Electronic Equipment" (Emerald Book). Section 9, "Uninterruptible Power Supply (UPS) Systems," discusses how UPS specifications, including battery runtime, are selected based on the nature of expected power disturbances. Ongoing adequacy requires monitoring these disturbances to ensure the selected solution remains appropriate.

3. University of Washington, "Uninterruptible Power Supply (UPS) FAQ." This document explains that a UPS's primary function is to provide "ride-through" time during short outages. The adequacy of the UPS is determined by whether its battery capacity can outlast the typical outage duration. (Available at: itconnect.uw.edu/learn/workshops/online-tutorials/ups-faq/)

Question: 26

Which of the following techniques would provide the BEST assurance to an IS auditor that all necessary data has been successfully migrated from a legacy system to a modern platform?

A: Review of logs from the migration process

B: Data analytics

C: Interviews with migration staff

D: Statistical sampling

Correct Answer:

B

Explanation:

Data analytics provides the most comprehensive and direct assurance for a successful data migration. By applying techniques such as reconciling record counts, comparing control totals (e.g., sums of numeric fields), and validating hash totals between the source and target systems, an auditor can verify both the completeness (all data was transferred) and the integrity (data was not altered) of the migrated data. This direct comparison of the final data state offers a higher level of assurance than other methods that only examine the process or a subset of the data.

Why Incorrect Options are Wrong:

A: Review of logs from the migration process: While useful for identifying errors, logs primarily verify that the migration process executed. They provide less direct assurance about the final data's integrity and completeness compared to direct data comparison.

C: Interviews with migration staff: This provides subjective, testimonial evidence. It is not a verifiable or reliable method for confirming that all data was migrated completely and accurately.

D: Statistical sampling: This method only examines a subset of the data. By definition, it cannot provide assurance that all necessary data has been successfully migrated, which is a key requirement of the question.

References:

1. ISACA, CISA Review Manual, 27th Edition. In Domain 3, Section 3.5.5 "Data Conversion," the manual emphasizes the need for auditors to verify that "reconciliation procedures are in place to verify that all data have been converted." These reconciliation procedures are a core component of data analytics.

2. ISACA Journal, "Auditing Data Migration," Volume 6, 2016. This article states, "The most important task is to verify that the data migration was successful... This can be done by comparing record counts and by spot-checking critical data fields both pre- and postmigration." This describes data analytics techniques for validation. (Available via ISACA membership portal).

3. IEEE Xplore, "A Framework for Validating Migrated Data in Database System," 2017 International Conference on Inventive Computing and Informatics (ICICI). This paper discusses validation techniques post-migration, stating, "The validation process involves comparing the source and target data... to check for completeness, correctness, and consistency." This academic source confirms that direct data comparison (analytics) is the standard for validation. (URL: https://ieeexplore.ieee.org/document/83 inventive computing and informatics icici/)

Question: 27

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: Regularly update business impact assessments

B: Prepare detailed plans for each business function.

C: Involve staff at all levels in periodic paper walk-through exercises

D: Make senior managers responsible for their plan sections.

Correct Answer:

C

Explanation:

The most effective method to ensure a Business Continuity Plan (BCP) will function as intended is through regular testing and exercises. A paper walk-through, a type of tabletop exercise, involves staff at all levels discussing their roles and responsibilities according to the plan. This process is critical for validating the plan's accuracy, identifying procedural gaps, and ensuring that personnel who must execute the plan are familiar with their duties. Testing transforms the BCP from a static document into a workable, understood procedure, providing the highest level of assurance of its effectiveness in a real disaster.

Why Incorrect Options are Wrong:

A: Regularly updating the business impact assessment (BIA) is a foundational input for the BCP, but it does not validate the plan's operational execution.

B: Preparing detailed plans is a necessary step, but without testing, there is no assurance that the documented procedures are practical or effective.

D: Senior management responsibility is crucial for governance and resource allocation but does not, by itself, ensure the plan is workable or that staff are prepared.

References:

1. ISACA, CISA Review Manual, 27th Edition. Domain 4: Information Systems Operations and Business Resilience. The manual states, "The purpose of BCP testing is to ensure that the BCP is viable and that the enterprise is prepared to execute the plan." It identifies walk-throughs (tabletop exercises) as a key testing method to ensure team members are familiar with the plan and their roles.

2. National Institute of Standards and Technology (NIST), Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. Section 5, "Contingency Plan Testing, Training, and Exercises," emphasizes that "Testing and exercises are the most thorough means of validating the viability of a contingency plan." It describes tabletop exercises as a common method to "validate the content of plans." (p. 41).

3. Goodman, M. (2014). The Official (ISC)² Guide to the CISSP CBK. Auerbach Publications. Chapter 17, "Business Continuity and Disaster Recovery Planning," explains that plan testing, including tabletop exercises, is essential to "ensure that the BCP will actually work when needed." It highlights that such exercises validate the plan and train the team.

Question: 28

Which ofthe following should be the PRIMARY concern of an IS auditor during a review of an external IT service level agreement (SLA) for computer operations?

A: Changes in services are nottracked

B: Vendor has exclusive control of IT resources

C: Lack of software escrow provisions

D: No employee succession plan

Correct Answer:

A

Explanation:

The primary purpose of a service level agreement (SLA) is to define and monitor the agreed-upon service levels. If changes to the services, scope, or performance metrics are not formally tracked through a change management process, the SLA becomes unenforceable. This prevents the organization from verifying vendor compliance, measuring performance against established baselines, and holding the vendor accountable for deviations. For an IS auditor, this is the most critical flaw as it undermines the fundamental control objective of the SLA itself.

Why Incorrect Options are Wrong:

B: Vendor has exclusive control of IT resources: This is an inherent characteristic of many outsourcing arrangements, not a flaw in the SLThe SLA is the primary control used to manage the risks associated with this model.

C: Lack of software escrow provisions: Software escrow is a specific control for mitigating risks related to vendor viability for licensed software, not a universal requirement for all computer operations services.

D: No employee succession plan: This is an internal operational concern for the vendor. The SLA should focus on service continuity outcomes (e.g., availability), not the vendor's specific internal HR processes.

References:

1. ISACA, CISA Review Manual, 27th Edition. In the context of IT service provider management, the manual emphasizes that SLAs must contain clear service definitions,

performance standards, and a formal process for managing changes. The absence of change tracking makes performance monitoring, a key audit objective, impossible. (Domain 2: Governance and Management of IT).

2. ISACA, COBIT 2019 Framework: Governance and Management Objectives. The management objective APO10, Managed Vendors, includes the key practice APO10.04, "Monitor vendor performance and compliance." This practice states, "Periodically review vendor performance against targets... and address deviations." This review is impossible if service changes are not tracked.

3. Tiwana, A., & Bush, (2005). A CMM-based framework for managing offshore outsourcing of software development. Information Systems Management, 22(2), 77-86. While focused on software, the principles apply broadly. The article highlights that effective outsourcing relationships require robust processes for "monitoring and controlling" the engagement, which fundamentally includes managing and tracking changes to the scope of work and service levels.

Question: 29

Which of the following would provide the BEST evidence for use in a forensic investigation of an employee's hard drive?

A: Prior backups

B: Bit-stream copy of the hard drive

C: A file level copy of the hard drive

D: Memory dump to an external hard drive

Correct Answer:

B

Explanation:

A bit-stream copy, also known as a forensic image, is a bit-for-bit replica of the entire hard drive. This method captures all data, including active files, deleted files residing in unallocated space, file slack, and system areas that are inaccessible through the operating system. This comprehensive and unaltered duplication is the cornerstone of digital forensics as it preserves the integrity of the original evidence, allowing for a thorough investigation without modifying the source media. It is the most complete and legally defensible evidence that can be collected from a hard drive.

Why Incorrect Options are Wrong:

A: Prior backups are incomplete as they represent a past state of the drive and typically do not include deleted files or other forensic artifacts.

C: A file level copy is inadequate because it only duplicates active files, completely missing deleted data, unallocated space, and slack space critical for forensic analysis.

D: Memory dump captures the contents of volatile RAM, not the data stored on the hard drive, making it irrelevant for investigating the hard drive itself.

References:

1. National Institute of Standards and Technology (NIST). (2006). Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response. Section 3.2.2, "Creating a Duplicate Image," states, "Creating a bit-stream image of the original media is a critical step... A bit-stream image is a bit-for-bit copy of the original media." (p. 21). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

2. ISAC(2019). CISA Review Manual, 27th Edition. Domain 5: Protection of Information Assets. The manual emphasizes that for forensic purposes, a bit-by-bit or bit-stream copy of a disk is necessary to ensure all data, including deleted files and ambient data, is captured for evidence.

3. Purdue University Global. (n.d.). IT420: Computer Forensics Course. Course materials frequently emphasize the distinction between a logical (file-level) copy and a physical (bit-stream) image, identifying the bit-stream image as the only acceptable method for creating a forensic duplicate of a storage device.

Question: 30

Which ofthe following is MOST likely to be detected by an IS auditor applying data analytic techniques?

A: Potentially fraudulent invoice payments originating within the accounts payable department

B: Completion of inappropriate cross-border transmission of personally identifiable information (PII)

C: Unauthorized salary or benefit changes to the payroll system generated by authorized users

D: Issues resulting from an unsecured application automatically uploading transactions to the general ledger

Correct Answer:

A

Explanation:

Data analytic techniques are most effective when applied to large, structured datasets to identify anomalies, outliers, and patterns that may indicate control weaknesses or fraud. Analyzing the entire population of accounts payable transactions is a classic and highly effective use of data analytics. An IS auditor can programmatically search for indicators of fraud such as duplicate invoice numbers, duplicate payments, payments to vendors with employee addresses, or payments just below an authorization threshold. These are patterns inherent within the transaction data itself, making them highly likely to be detected.

Why Incorrect Options are Wrong:

B: Detecting inappropriate cross-border data transmission typically requires specialized Data Loss Prevention (DLP) tools or deep packet inspection of network traffic, not just analysis of a standard transactional dataset.

C: While analytics can flag unusual salary changes, determining if a change made by an authorized user was unauthorized requires external verification (e.g., HR approval forms), which is outside the scope of analyzing the payroll data alone.

D: Data analytics on the general ledger might reveal symptoms (e.g., erroneous entries), but it would not directly identify the root cause as being an "unsecured application." This requires a technical configuration or application review.

References:

1. ISACA, CISA Review Manual, 27th Edition. Chapter 1, "The Information System Auditing Process," details the use of Computer-Assisted Audit Techniques (CAATs) and data analytics. It explicitly lists examples such as "identifying duplicate payments" and "identifying gaps in check or invoice number sequences," which are directly applicable to detecting accounts payable fraud.

2. Nigrini, M. J. (2011). Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations. John Wiley & Sons. Chapter 5, "The Procure-to-Payment Cycle," extensively covers data analytic tests for detecting fraudulent invoice payments, reinforcing that this is a primary application area.

3. ISAC(2014). Data Analytics - A Practical Approach. This guide provides numerous examples of using data analytics in audits, with a significant focus on analyzing transactional data from financial systems like accounts payable to detect fraud and errors. (Referenced in various ISACA Journal articles and white papers).