CISA Domain 1 Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **The extent of data collection during an IS audit should be determined primarily by what factor?**
   - **A. Availability of critical information**
   - **B. Auditor's familiarity with the circumstances**
   - **C. Auditee's ability to find relevant evidence**
   - **D. Purpose and scope of the audit**

2. **What is a key attribute of the control self-assessment approach?**
   - **A. Broad stakeholder involvement.**
   - **B. Auditors are the primary control analysts.**
   - **C. Limited employee participation.**
   - **D. Policy driven.**

3. **What is an IS auditor's responsibility when evaluating software development practices?**
   - **A. To verify project manager's decisions**
   - **B. To analyze interactions between QA and project management**
   - **C. To assess coding efficiency**
   - **D. To ensure compliance with coding standards**

4. **The main purpose of the annual IS audit plan is to:**
   - **A. Allocate resources for audits**
   - **B. Reduce the impact of audit risk**
   - **C. Develop a training plan for auditors**
   - **D. Minimize audit costs**

5. **Which action is NOT an effective compensating control when segregation of duties cannot be implemented?**
   - **A. Logging of changes to critical functions**
   - **B. Conducting regular access reviews**
   - **C. Implementing additional management oversight**
   - **D. Restricting system access to only one user**

6. Which audit technique can find flaws but might not identify overlapping controls?

A. Review of documentation

B. Integrated test facility

C. Manual testing of controls

D. Automated monitoring solutions

7. What should be the primary concern if an IS auditor discovers a lack of segregation of duties?

A. Implementing compensating controls

B. Enhancing the auditing process

C. Reporting the condition

D. Recommending training for staff

8. In the context of IS audits, what does adequate evidence rely primarily on?

A. The processes and personnel who author the data

B. The priority of risk assessments conducted

C. The number of audit findings reported

D. The training of audit staff involved

9. In a scenario of high inherent and control risk, what additional audit action is typically warranted?

A. Compliance testing

B. Substantive testing

C. Discovery sampling

D. Stop-or-go sampling

10. After identifying a business process for an audit, what should the IS auditor identify NEXT?

A. Most valuable information assets

B. IS audit resources to be deployed

C. Auditee personnel to be interviewed

D. Control objectives and activities

Answers

1. D
2. A
3. B
4. A
5. D
6. B
7. C
8. A
9. B
10. D

Explanations

1. The extent of data collection during an IS audit should be determined primarily by what factor?

A. Availability of critical information

B. Auditor's familiarity with the circumstances

C. Auditee's ability to find relevant evidence

D. Purpose and scope of the audit

The extent of data collection during an information systems audit is fundamentally guided by the purpose and scope of the audit. This factor defines the specific objectives that the audit seeks to accomplish, which in turn dictates what data is necessary to adequately assess and evaluate the information systems in question. Understanding the purpose and scope ensures that the audit is focused and relevant, allowing the auditor to align their efforts with organizational goals, compliance requirements, and risk assessments. For example, if the audit's objective is to evaluate compliance with regulatory requirements, the data collected will be more focused on that specific area. Conversely, if the purpose involves a comprehensive risk assessment, a broader range of data would be needed. In contrast, the availability of critical information, the auditor's familiarity with the circumstances, and the auditee's ability to find relevant evidence may influence the data collection process, but they do not fundamentally define the extent of data needed. The purpose and scope serve as the guiding principles to ensure that the audit remains efficient, effective, and aligned with its objectives.

2. What is a key attribute of the control self-assessment approach?

A. Broad stakeholder involvement.

B. Auditors are the primary control analysts.

C. Limited employee participation.

D. Policy driven.

A control self-assessment approach emphasizes broad stakeholder involvement as a key attribute because it encourages input and participation from various levels within the organization. This inclusive approach allows for diverse perspectives, which enhances the understanding of risks and controls across different departments and functions. By engaging a wider range of stakeholders, the organization can better identify control strengths and weaknesses, facilitating a more thorough evaluation of existing processes. This participatory model not only promotes accountability but also fosters a culture of continuous improvement, as employees at all levels become more aware of their roles in the control environment. In contrast, focusing solely on auditors or limiting employee participation would likely reduce the effectiveness of the assessment by missing insights from those directly engaged with the processes being evaluated. Similarly, being solely policy-driven might risk overlooking practical, real-world applications and insights that emerge from direct employee involvement. Overall, broad stakeholder involvement is crucial in making control self-assessments comprehensive and effective.

3. What is an IS auditor's responsibility when evaluating software development practices?

A. To verify project manager's decisions

B. To analyze interactions between QA and project management

C. To assess coding efficiency

D. To ensure compliance with coding standards

When evaluating software development practices, an IS auditor plays a crucial role in analyzing interactions between quality assurance (QA) and project management. This responsibility is significant because effective communication and coordination between these two areas are vital for the successful delivery of software projects. Quality assurance is responsible for ensuring that the software meets specified requirements and is free from defects. On the other hand, project management focuses on managing timelines, resources, and project scopes. By examining how these groups interact, an auditor can identify potential issues or inefficiencies that could affect the quality and success of the software development process. For instance, if QA is not adequately involved early in the project management process, there may be a higher risk of releasing subpar products or requiring costly revisions later on. This evaluation also helps ensure that best practices are followed, promoting a culture of quality and accountability throughout the software development lifecycle. Thus, understanding and analyzing the dynamics between QA and project management aids in identifying opportunities for improvement and risk management in the software development process.

4. The main purpose of the annual IS audit plan is to:

A. Allocate resources for audits

B. Reduce the impact of audit risk

C. Develop a training plan for auditors

D. Minimize audit costs

The primary objective of an annual IS audit plan is to allocate resources effectively for audits. This involves determining which areas of the information systems require attention based on their risk assessments, compliance requirements, and strategic objectives of the organization. By prioritizing and scheduling audits, the plan ensures that the internal audit function can allocate the appropriate number of skilled auditors, time, and other necessary resources to assess risk areas comprehensively. Resource allocation is crucial for optimizing audit operations, as it enables the audit team to focus on high-risk areas and ensure that audits are conducted in a timely manner. This planning process not only supports thorough examinations of controls and processes but also enhances the overall audit effectiveness and efficiency, leading to more reliable conclusions about the organization's information systems. The other options, while relevant to certain aspects of auditing, do not capture the main purpose of the IS audit plan as effectively. For instance, reducing audit risk or minimizing costs may occur as indirect benefits of proper resource allocation, but they are not the fundamental goal of the plan itself. Similarly, developing a training plan for auditors is important but falls under operational improvement rather than a primary purpose of the audit plan.

5. Which action is NOT an effective compensating control when segregation of duties cannot be implemented?

A. Logging of changes to critical functions

B. Conducting regular access reviews

C. Implementing additional management oversight

D. Restricting system access to only one user

Restricting system access to only one user is not an effective compensating control when segregation of duties cannot be implemented because it can lead to a single point of failure and increased risk of fraud or error. By giving only one user access to critical functions, you reduce the opportunities for checks and balances that come from having multiple individuals involved in processes. Segregation of duties is designed to ensure that no single individual has control over all aspects of a transaction, which inherently limits the potential for unintentional mistakes or malicious actions. Effective compensating controls, on the other hand, should promote oversight, accountability, and transparency, which is lacking in a one-user scenario. In contrast, actions such as logging changes, conducting regular access reviews, and implementing additional management oversight are all essential practices that help to monitor activities and provide a level of control despite the limitations posed by lack of segregation. These methods ensure that there is a record of actions taken, regular evaluations of who has access to what, and that there is an additional layer of scrutiny from management, all of which contribute to stronger governance and risk management.

6. Which audit technique can find flaws but might not identify overlapping controls?

A. Review of documentation

B. Integrated test facility

C. Manual testing of controls

D. Automated monitoring solutions

The integrated test facility is a technique used during audits that incorporates a simulated environment, allowing auditors to conduct test transactions within the same system environment as real transactions. This approach is valuable because it enables auditors to assess the functioning of controls in real-time alongside operational processes. While integrated test facilities can effectively reveal flaws in controls or processes because they mimic real-world conditions, they might not always identify overlapping controls—situations where multiple controls serve the same purpose or risk. Since the focus of this technique is generally on testing specific functions or processes, it may not provide a comprehensive view of all controls within the system, especially overlapping ones that might not be tested directly in the simulated environment. In contrast, reviewing documentation focuses on established procedures and protocols and can uncover a broader range of control descriptions, making it easier to identify overlaps. Manual testing of controls typically involves checking individual controls in detail, which can also highlight redundancies. Automated monitoring solutions continuously evaluate and report on controls but may not be specifically designed to test for overlaps.

7. What should be the primary concern if an IS auditor discovers a lack of segregation of duties?

A. Implementing compensating controls

B. Enhancing the auditing process

C. Reporting the condition

D. Recommending training for staff

The primary concern when an IS auditor discovers a lack of segregation of duties is to report the condition. Segregation of duties is a fundamental internal control that helps prevent fraud and errors by ensuring that no single individual has control over all aspects of any critical business process. When this control is absent, there is an increased risk of unauthorized actions, as an individual can both perform and approve tasks. Reporting the condition is critical because it alerts management and the relevant stakeholders to the control weakness, enabling them to take necessary actions to mitigate risks. This communication is essential for risk management and ensuring the integrity of financial reporting and operational processes. It is often a prerequisite for any follow-up actions or recommendations to be made. While implementing compensating controls, enhancing the auditing process, and recommending training are all important actions that could follow the discovery of such a deficiency, the immediate priority lies in reporting the risk so that it can be addressed promptly.

8. In the context of IS audits, what does adequate evidence rely primarily on?

A. The processes and personnel who author the data

B. The priority of risk assessments conducted

C. The number of audit findings reported

D. The training of audit staff involved

In the context of Information Systems audits, adequate evidence is primarily dependent on the processes and personnel who author the data. This emphasis on the origin of data underscores the importance of ensuring that the information being assessed is credible and reliable. When data is created or manipulated by well-defined processes and competent personnel, it has a higher likelihood of being accurate and trustworthy. The integrity of evidence is fundamentally connected to the competence of those who generate it and the robustness of the processes in place. Auditors must be able to trace the evidence back to competent sources to establish a solid foundation for their audit findings. This relationship helps to support assertions and conclusions drawn during the audit process, ensuring that decisions made based on the audit are sound and based on high-quality data. While the other options may have their own relevance in the audit process—risk assessment prioritization can help guide audit focus, a high number of audit findings could indicate underlying issues, and the training of audit staff is critical for effective execution of audits—they do not impact the foundational validity and reliability of the evidence as directly as the processes and personnel responsible for the data itself.

9. In a scenario of high inherent and control risk, what additional audit action is typically warranted?

A. Compliance testing

B. Substantive testing

C. Discovery sampling

D. Stop-or-go sampling

In a scenario characterized by high inherent and control risk, conducting substantive testing is generally warranted. This type of testing involves verifying the accuracy and completeness of account balances and transactions, as opposed to simply evaluating the design and effectiveness of internal controls. When inherent risk is high, it indicates that the nature of the accounts or transactions being audited is more likely to misstate financial statements. Control risk reflects the possibility that the controls in place may fail to prevent or detect misstatements. In such situations, auditors need to provide more substantial evidence to support their conclusions. Substantive testing serves this purpose by directly assessing the underlying data through tests of details or analytical procedures, thus allowing the auditor to form a more reliable opinion on the financial statements. It's important to note that while compliance testing assesses adherence to laws and regulations and the effectiveness of internal controls, it may not provide the level of assurance needed when risks are elevated. Techniques like discovery sampling and stop-or-go sampling are more specific approaches to sampling and are generally used in different contexts. Therefore, substantive testing becomes the most appropriate action for addressing the increased uncertainty associated with high risk situations.

10. After identifying a business process for an audit, what should the IS auditor identify NEXT?

A. Most valuable information assets

B. IS audit resources to be deployed

C. Auditee personnel to be interviewed

D. Control objectives and activities

Following the identification of a business process for an audit, the most logical next step is to define the control objectives and activities. This is critical because understanding the control objectives helps the auditor determine what the audit aims to assess regarding the effectiveness and efficiency of the controls governing the business process. Control objectives specify what needs to be achieved through the controls in place, providing a framework for evaluating whether the business process operates as intended. Identifying these objectives allows the auditor to create a structured approach to assess the reliability of the system, compliance with regulations, and the safeguarding of assets. In subsequent steps, the auditor may indeed consider valuable information assets, audit resources, and personnel interviews, but these elements become useful only after the control objectives have been established. This sequence ensures that the audit process is focused and relevant, allowing for a deeper understanding of the specific controls that need to be examined for effectiveness and alignment with the organization's goals.