# CISA Domain 2 Practice Exam (Sample)

## Study Guide


**Everything you need from our exam experts!**

# Questions

1. **Which method best supports the prioritization of new IT projects?**
   - **A. Internal control self-assessment**
   - **B. Information systems audit**
   - **C. Investment portfolio analysis**
   - **D. Business risk assessment**

2. **In the context of IT strategic planning, what is essential for the plan to articulate?**
   - **A. State-of-the-art technology implementation**
   - **B. The organization's mission and vision for IT**
   - **C. Specific project management practices**
   - **D. Operational control measures**

3. **Which of the following is the best practice for ensuring compliance in IT policies?**
   - **A. Regular updates of all IT policies**
   - **B. Ensuring management approval of policies**
   - **C. Involving all departments in policy creation**
   - **D. Providing training for all employees**

4. **During a risk management review, what is the most important consideration?**
   - **A. Controls are implemented based on cost-benefit analysis**
   - **B. The risk management framework is based on global standards**
   - **C. The approval process for risk response is in place**
   - **D. IT risk is presented in business terms**

5. **How can an organization best ensure its policies are effective in guiding legal compliance?**
   - **A. Periodic training for all employees**
   - **B. Regular updates to policies based on changes in laws**
   - **C. Inclusion of specific examples in each policy**
   - **D. Periodic review by experts in legal compliance**

**6. What primary concern should an IS auditor have regarding compliance with IT governance?**

**A. Compliance with international regulations**

**B. Alignment of IT objectives with business objectives**

**C. Implementation of security protocols**

**D. Adequate workforce training**

**7. How should segregation of duties be enforced in a scenario with only one DBA having root access?**

**A. Hire a second DBA and split the duties between the two individuals**

**B. Remove the DBA's root access on all UNIX servers**

**C. Ensure that all actions of the DBA are logged and that all logs are backed up to tape**

**D. Ensure that database logs are forwarded to a UNIX server where the DBA does not have root access**

**8. What composition should an IT steering committee ideally have?**

**A. A mix of members from different departments and staff levels**

**B. Only senior management members**

**C. A majority of IT staff**

**D. Frequent turnover of members**

**9. When reviewing a quality management system, what should the IS auditor primarily focus on collecting evidence for?**

**A. Quality management systems comply with good practices**

**B. Continuous improvement targets are being monitored**

**C. Standard operating procedures are updated annually**

**D. Key performance indicators are defined**

**10. What concern should an IS auditor prioritize when reviewing an organization's governance model?**

**A. The information security policy is not reviewed**

**B. A policy for timely system patching does not exist**

**C. The audit committee did not review the mission statement**

**D. No policy related to information asset protection exists**

# Answers

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

# Explanations

## 1. Which method best supports the prioritization of new IT projects?

**A. Internal control self-assessment**

**B. Information systems audit**

**C. Investment portfolio analysis**

**D. Business risk assessment**

**Investment portfolio analysis is the most effective method for prioritizing new IT projects because it focuses on evaluating and comparing the potential returns and risks associated with various investments. This approach allows organizations to align their IT projects with overall business objectives and allocate resources efficiently. By analyzing the expected benefits, costs, and strategic importance of each project, decision-makers can prioritize initiatives that will provide the most value and support the organization's goals. This method also considers the interdependencies between projects, allowing for a comprehensive view of how investments can be optimized within the entire portfolio. It facilitates informed decision-making by quantifying the trade-offs involved in different project options, leading to better management of limited resources and strategic alignment. This structured evaluation can help organizations avoid over-investing in less impactful projects while ensuring that high-priority initiatives receive the necessary support and funding.**

## 2. In the context of IT strategic planning, what is essential for the plan to articulate?

**A. State-of-the-art technology implementation**

**B. The organization's mission and vision for IT**

**C. Specific project management practices**

**D. Operational control measures**

**Articulating the organization's mission and vision for IT is crucial in IT strategic planning because it ensures that all technology initiatives align with the overarching goals and objectives of the organization. By clearly stating the mission and vision, the strategic plan provides a framework that guides decisions about technology investments and prioritization. This alignment fosters a better understanding among stakeholders of how IT can support and enhance business operations and strategy, ultimately driving the organization toward its long-term goals. Having a clear mission and vision for IT enables stakeholders to make informed decisions regarding technology adoption, resource allocation, and project prioritization. It also helps in communicating the purpose of IT within the organization, fostering buy-in from both leadership and employees. In contrast, while state-of-the-art technology implementation and specific project management practices are important components of technology plans, they must be rooted in a clear organizational direction to ensure they contribute effectively to overall success. Similarly, operational control measures, although valuable for day-to-day management, do not encapsulate the strategic direction that a mission and vision provide.**

## 3. Which of the following is the best practice for ensuring compliance in IT policies?

**A. Regular updates of all IT policies**

**B. Ensuring management approval of policies**

**C. Involving all departments in policy creation**

**D. Providing training for all employees**

**Ensuring management approval of policies is a foundational aspect of establishing compliance within an organization's IT governance framework. When management reviews and approves IT policies, it signifies a commitment to uphold those policies across the organization. This top-down approach not only reinforces the authority and legitimacy of the policies but also facilitates necessary resource allocation and alignment with business objectives. Management involvement ensures that policies reflect the organization's risk tolerance, regulatory requirements, and strategic goals. This approval process can significantly enhance buy-in from employees, as it indicates that leadership supports and prioritizes these guidelines, fostering a culture of compliance throughout the organization. While regular updates, involvement of all departments, and employee training are essential elements of an effective policy management program, without official management approval, the policies may lack the necessary authority or support needed for successful implementation and adherence.**

## 4. During a risk management review, what is the most important consideration?

**A. Controls are implemented based on cost-benefit analysis**

**B. The risk management framework is based on global standards**

**C. The approval process for risk response is in place**

**D. IT risk is presented in business terms**

**The most important consideration during a risk management review is that IT risk is presented in business terms. This is crucial because it ensures that the risks associated with information technology are communicated effectively to stakeholders who may not have a technical background, such as senior management or the board of directors. By articulating IT risks in business terms, you can emphasize their potential impact on organizational objectives, help prioritize risk responses based on business needs, and facilitate informed decision-making. When IT risks are framed in a way that aligns with business goals, it drives home the importance of risk management in protecting the organizational strategy and resources. It also promotes a better understanding of the implications of the risk and can lead to increased support for necessary risk mitigation strategies. While implementing controls based on cost-benefit analysis, adhering to global standards, and having a solid approval process for risk response are all important components of a robust risk management framework, they ultimately rely on the effective communication of IT risks in terms that resonate with business stakeholders. If the business leaders do not grasp the significance of the IT risks, they may overlook or undervalue crucial aspects of risk management that are essential for safeguarding the organization's assets and achieving its objectives.**

## 5. How can an organization best ensure its policies are effective in guiding legal compliance?

**A. Periodic training for all employees**

**B. Regular updates to policies based on changes in laws**

**C. Inclusion of specific examples in each policy**

**D. Periodic review by experts in legal compliance**

**To ensure policies are effective in guiding legal compliance, periodic review by experts in legal compliance is crucial. This practice allows organizations to stay aligned with current laws and regulations, which can frequently change. Experts possess the knowledge and skills necessary to interpret legal requirements and assess whether organizational policies adequately reflect these obligations. A thorough review by professionals can identify any potential gaps or outdated provisions within existing policies, leading to necessary updates and adjustments. It ensures that policies not only comply with the law but also reflect best practices in the industry. Without expert insights, policies may become ineffective, leading to potential legal risks and liabilities. While periodic training for employees, regular updates based on legal changes, and including specific examples can all contribute to the understanding and implementation of policies, they are secondary to having a framework that is consistently evaluated by legal experts. Their specialized knowledge ensures that policies are relevant and comprehensive in addressing compliance requirements effectively.**

## 6. What primary concern should an IS auditor have regarding compliance with IT governance?

**A. Compliance with international regulations**

**B. Alignment of IT objectives with business objectives**

**C. Implementation of security protocols**

**D. Adequate workforce training**

**The primary concern for an IS auditor regarding compliance with IT governance centers around the alignment of IT objectives with business objectives. This alignment is crucial because IT governance is fundamentally about ensuring that IT investments and operations support and enhance the overall business goals of the organization. When IT objectives are in sync with business objectives, it leads to improved performance, better resource allocation, and increased value from technology investments. This alignment ensures that IT strategies are not only focused on technological advancements but also consider the needs and requirements of the business. Without this synergy, there is a risk that IT initiatives will not deliver the expected benefits or address key business challenges, ultimately hindering the organization's capacity to meet its strategic goals. An IS auditor's role often includes assessing whether the governance framework properly integrates IT functions with the business strategy, thus reinforcing the importance of this alignment. While other options, such as compliance with international regulations, implementation of security protocols, and adequate workforce training, are important factors in a broader context, they serve as supporting aspects of the more critical, overarching goal of ensuring that IT resources and efforts contribute effectively to the business's objectives.**

## 7. How should segregation of duties be enforced in a scenario with only one DBA having root access?

**A. Hire a second DBA and split the duties between the two individuals**

**B. Remove the DBA's root access on all UNIX servers**

**C. Ensure that all actions of the DBA are logged and that all logs are backed up to tape**

**D. Ensure that database logs are forwarded to a UNIX server where the DBA does not have root access**

**The correct approach to enforce segregation of duties in a scenario where there is only one DBA with root access is to ensure that database logs are forwarded to a UNIX server where the DBA does not have root access. This method strengthens security by creating an oversight mechanism that limits the DBA's ability to alter or tamper with logs that could otherwise provide evidence of actions taken within the system. By forwarding the database logs to a separate UNIX server, you minimize the risk associated with having a single individual with unrestricted access. This separation ensures that even if the DBA performs actions that might be considered unauthorized, there is an independent source of logging that cannot be modified by the DBA. This helps maintain the integrity of the audit trail, which is essential for accountability and compliance with various regulations. In contrast, hiring a second DBA to split duties might not be feasible in all organizations and can come with additional costs and complexities. Simply removing the DBA's root access could hinder legitimate administrative functions necessary for maintaining the database environment. Ensuring that all actions of the DBA are logged and backing up those logs, while important, does not provide the same level of control and oversight as forwarding logs to a server with restricted access for the DBA. Thus, option D presents the most effective means of implementing**

## 8. What composition should an IT steering committee ideally have?

**A. A mix of members from different departments and staff levels**

**B. Only senior management members**

**C. A majority of IT staff**

**D. Frequent turnover of members**

**An effective IT steering committee ideally includes a mix of members from different departments and staff levels. This composition allows for diverse perspectives and helps ensure that IT initiatives align with the organization's goals and strategies. Representatives from various departments can provide insights into their specific needs and challenges, leading to more effective decision-making and prioritization of IT projects. Having a committee made up only of senior management members may limit the scope of understanding and consideration of frontline operational challenges. It can result in a disconnect between IT plans and the actual needs of the departments that rely on technology for daily operations. Similarly, having a majority of IT staff would narrow the focus solely to technical perspectives, overlooking essential input from other areas of the business. Frequent turnover of members would also disrupt continuity and hinder the committee's ability to develop a cohesive strategy, making the establishment of long-term goals more difficult. Therefore, a well-rounded committee composition that reflects different levels and functional areas within the organization is essential for the success of IT governance.**

## 9. When reviewing a quality management system, what should the IS auditor primarily focus on collecting evidence for?

**A. Quality management systems comply with good practices**

**B. Continuous improvement targets are being monitored**

**C. Standard operating procedures are updated annually**

**D. Key performance indicators are defined**

**Focusing on continuous improvement targets as the primary evidence in a quality management system review is essential due to its direct impact on the effectiveness and efficiency of processes. Continuous improvement signifies a commitment to ongoing enhancement of products, services, or processes, which is a fundamental principle in quality management. By monitoring these targets, an IS auditor can determine how well the organization is performing in terms of quality metrics and whether it is proactively seeking ways to improve. Additionally, the monitoring of continuous improvement targets can reveal insights into the organization's quality culture, its responsiveness to feedback, and its adaptability to changes in the market or industry standards. Evidence in this area can shed light on whether the management system is dynamic and operationally effective, pointing to a commitment not just to maintain quality but to exceed standards through ongoing refinement. While compliance with good practices, updates of standard operating procedures, and definitions of key performance indicators all play significant roles in a quality management system, they are often more static and may not provide the same depth of insight into the organization's commitment to improvement as continuous monitoring of improvement targets does. The focus on continuous improvement inherently encompasses the need for compliance, updates, and performance definitions, making it a more comprehensive area for the auditor to examine.**

## 10. What concern should an IS auditor prioritize when reviewing an organization's governance model?

**A. The information security policy is not reviewed**

**B. A policy for timely system patching does not exist**

**C. The audit committee did not review the mission statement**

**D. No policy related to information asset protection exists**

**When reviewing an organization's governance model, a primary concern for an IS auditor is the review and maintenance of the information security policy. An effective governance model relies on having up-to-date policies that outline how an organization manages its information security risks. If the information security policy is not regularly reviewed, it could become outdated and fail to address current threats, regulatory requirements, and business objectives. This could lead to inadequate protection of the organization's assets and increased vulnerability to security breaches. Moreover, the information security policy serves as a critical framework for guiding the organization's overall security practices and ensuring compliance with relevant standards. Prioritizing the review of this policy aligns with the fundamental goal of governance, which is to ensure that the organization is effectively managed and that risk is appropriately mitigated. In this context, having an unreviewed policy signifies a potential oversight that could compromise the effectiveness of the entire governance structure.**