CISA DOMAIN 5 PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cisadomain5.examzify.com

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **What is the PRIMARY concern of an IS auditor when a service provider outsources part of its work?**

   A. Contract termination due to lack of permission

   B. Confidentiality of the information can be compromised

   C. Subsequent suppliers not being subject to audit

   D. Direct approaches from the outsourcer to the secondary provider

2. **What document is crucial for ensuring security upon an employee's exit from the organization?**

   A. Exit interview documentation

   B. Job rotation requirement

   C. Termination checklist

   D. Nondisclosure agreements

3. **How does a responsible, accountable, consulted, and informed (RACI) chart support IT initiatives?**

   A. By facilitating team bonding sessions

   B. By clarifying roles and responsibilities

   C. By managing project timelines

   D. By monitoring stakeholder feedback

4. **If an organization's management decides to keep information security investments inadequate due to profitability pressure, what should an IS auditor recommend?**

   A. Use cloud providers for low-risk operations.

   B. Revise compliance enforcement processes.

   C. Request that senior management accept the risk.

   D. Postpone low-priority security procedures.

5. **To minimize risks associated with short-term employees, which activity should an IS audit department include?**

   A. Succession planning

   B. Staff job evaluation

   C. Responsibilities definitions

   D. Employee award programs

6. What should an IS auditor recommend to best enforce alignment of an IT project portfolio with strategic priorities?

A. Define a balanced scorecard for measuring performance

B. Consider user satisfaction in key performance indicators

C. Select projects according to business benefits and risk

D. Modify the yearly process of defining the project portfolio

7. Which risk management practice is most likely to expose an organization to compliance risk?

A. Risk reduction

B. Risk transfer

C. Risk avoidance

D. Risk mitigation

8. What is the most appropriate recommendation for a call center that does not assign unique user accounts?

A. Have the current configuration approved by operations management

B. Ensure an audit trail for all existing accounts

C. Implement individual user accounts for all staff

D. Amend the IT policy to allow shared accounts

9. When a startup is handling software development for an enterprise, what should be recommended to ensure investment protection?

A. Due diligence on the software vendor

B. A quarterly audit of the vendor facilities

C. A source code escrow agreement

D. A high penalty clause in the contract

10. What should be the primary concern of an IS auditor reviewing external IT service provider management?

A. Minimizing costs for the services provided

B. Evaluating the process for transferring knowledge to the IT department

C. Prohibiting the provider from subcontracting services

D. Determining if the services were provided as contracted

Answers

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

Explanations

1. What is the PRIMARY concern of an IS auditor when a service provider outsources part of its work?

A. Contract termination due to lack of permission

B. Confidentiality of the information can be compromised

C. Subsequent suppliers not being subject to audit

D. Direct approaches from the outsourcer to the secondary provider

The primary concern of an IS auditor when assessing the outsourcing of work to a service provider revolves around the confidentiality of information. When an organization outsources tasks, especially those linked to sensitive data, there is an inherent risk that confidential information could be compromised. This concern stems from several factors, including the potential unauthorized access to or misuse of data by third-party vendors. Auditors are particularly focused on ensuring that adequate controls and safeguards are in place to protect this information during its handling by external parties. Confidentiality is a critical aspect of information security, as breaches can lead to financial losses, reputational damage, and legal consequences for the organization. Thus, the auditor must evaluate whether the service provider has effective measures and policies to maintain confidentiality throughout the outsourcing process, including any obligations placed on subsequent suppliers, access controls, employee training, and incident response plans. In contrast, while contract termination, auditing of subsequent suppliers, and direct approaches from the outsourcer to secondary providers are relevant issues, they typically focus on procedural or compliance aspects rather than the direct risk to the confidentiality of sensitive information, which is why the confidentiality concern takes precedence in the auditor's assessment.

2. What document is crucial for ensuring security upon an employee's exit from the organization?

A. Exit interview documentation

B. Job rotation requirement

C. Termination checklist

D. Nondisclosure agreements

The termination checklist is essential for ensuring security upon an employee's exit from the organization. This document serves as a comprehensive guide that outlines all the necessary steps and items that need to be addressed prior to an employee leaving. It typically includes actions such as recovering company property (like laptops and security badges), disabling access to systems, updating passwords, and conducting exit interviews. By following a well-structured termination checklist, the organization can effectively mitigate potential security risks. This includes preventing unauthorized access to sensitive data and systems by ensuring that the departing employee's access rights are revoked promptly. Moreover, the checklist helps to ensure that no critical protocols are overlooked, thus safeguarding the organization's assets and data integrity during the transition. In contrast, exit interview documentation is valuable for gathering feedback about the employee's experience but does not directly address security measures. Job rotation requirements are geared towards minimizing insider threats while an employee is still with the organization, rather than focusing on the exit process. Nondisclosure agreements protect sensitive information but are typically established at the start of employment, rather than being a specific procedure for when an employee departs. Thus, the termination checklist stands out as the most direct tool for ensuring security upon an employee's exit.

3. How does a responsible, accountable, consulted, and informed (RACI) chart support IT initiatives?

A. By facilitating team bonding sessions

B. By clarifying roles and responsibilities

C. By managing project timelines

D. By monitoring stakeholder feedback

A RACI chart supports IT initiatives primarily by clarifying roles and responsibilities within a project or team. This tool helps define who is Responsible for completing specific tasks, who is Accountable for ensuring tasks are completed, who should be Consulted (involved in discussions and decision-making), and who needs to be Informed about progress and updates. When roles and responsibilities are clearly defined, team members understand their duties and the expectations set upon them. This clarity helps to avoid confusion, overlaps, and gaps in work, which can lead to inefficiencies and delays in projects. By ensuring all team members know their contributions and how they relate to others, a RACI chart enhances collaboration and streamlines decision-making processes, ultimately leading to more effective IT initiatives. The other options, while they may contribute to a successful project environment in different ways, do not directly relate to the primary function of a RACI chart. For example, facilitating team bonding sessions focuses on interpersonal relationships, managing project timelines pertains to scheduling and deadlines, and monitoring stakeholder feedback involves understanding stakeholder perspectives, none of which are functions of role clarification inherent in a RACI chart.

4. If an organization's management decides to keep information security investments inadequate due to profitability pressure, what should an IS auditor recommend?

A. Use cloud providers for low-risk operations.

B. Revise compliance enforcement processes.

C. Request that senior management accept the risk.

D. Postpone low-priority security procedures.

When an organization's management chooses to maintain inadequate information security investments due to pressures related to profitability, the most appropriate recommendation for an IS auditor is to request that senior management accept the risk. This course of action acknowledges that the organization's decision to underinvest in security measures introduces specific risks that could impact its operations, data integrity, and reputation. By formally accepting the risk, senior management is made aware of the vulnerabilities and potential consequences that arise from not adequately securing information assets. This enables the organization to proceed with a clear understanding of the implications of their decision and ensures that there is a documented acknowledgment of the risks involved. It also facilitates better decision-making in the future, should the organization face security incidents or data breaches, as there is an established understanding that risks were identified, discussed, and accepted. Addressing the options in context, while using cloud providers for low-risk operations may mitigate certain risks, it doesn't address the broader implications of inadequate security investments across the organization. Revising compliance enforcement processes could enhance adherence to regulations but may not resolve the fundamental issue of insufficient security funding. Postponing low-priority security procedures, while it may seem like a temporary solution, fails to address the underlying risks associated with insufficient overall investment in cybersecurity. Thus, the appropriate recommendation

5. To minimize risks associated with short-term employees, which activity should an IS audit department include?

A. Succession planning

B. Staff job evaluation

C. Responsibilities definitions

D. Employee award programs

In the context of minimizing risks associated with short-term employees, focusing on succession planning is essential. Succession planning involves identifying and developing internal personnel to fill key positions within the organization as they become available. By ensuring there are trained staff members ready to take over, the organization mitigates the risks associated with turnover and short-term employment. Short-term employees may lack the depth of institutional knowledge or stability that long-term employees have, which can lead to disruptions in operations and project continuity. Having a robust succession plan allows an organization to ensure that critical knowledge, skills, and competencies are maintained even when short-term personnel are in play. This planning allows for smoother transitions and ensures that the organization continues to operate effectively despite fluctuations in employee tenure. In contrast, the other options do not directly address the specific risks posed by short-term employees. Staff job evaluations focus more on assessing performance rather than preparing for turnover, while defining responsibilities helps clarify roles but does not inherently prepare for employee exits. Employee award programs can boost morale but do not contribute to risk mitigation related to short-term employment. Therefore, focusing on succession planning specifically aligns with minimizing risks associated with this group of employees.

6. What should an IS auditor recommend to best enforce alignment of an IT project portfolio with strategic priorities?

A. Define a balanced scorecard for measuring performance

B. Consider user satisfaction in key performance indicators

C. Select projects according to business benefits and risk

D. Modify the yearly process of defining the project portfolio

Recommending that projects be selected according to business benefits and risk ensures that the IT project portfolio is closely aligned with strategic priorities. This approach emphasizes the importance of evaluating projects based on how they contribute to the organization's goals and the potential risks they may pose. By prioritizing projects that offer the highest business value while considering associated risks, an IS auditor helps ensure that resources are allocated efficiently and effectively, maximizing ROI and minimizing potential adverse effects on strategic initiatives. Selecting projects based on business benefits means that the organization can focus on initiatives that directly support its objectives. Considering risk further enhances this alignment by ensuring that the organization does not engage in high-risk projects that could detract from achieving its strategic goals or divert resources from lower-risk, high-value projects. This holistic approach to project selection is vital for maintaining a portfolio that not only supports the company's mission but also adapts to changing circumstances and priorities in the business environment.

7. Which risk management practice is most likely to expose an organization to compliance risk?

A. Risk reduction

B. Risk transfer

C. Risk avoidance

D. Risk mitigation

The practice of risk transfer involves shifting the responsibility for managing a particular risk to another party, typically through mechanisms like insurance or outsourcing certain operations. While risk transfer can alleviate immediate financial exposures, it can also increase compliance risk if the organization relies on the third party to maintain regulatory requirements or standards. If the third party fails to comply with regulations, the original organization may still be held liable, exposing it to potential legal penalties and reputational damage. In contrast, risk reduction aims to lower the likelihood or impact of risks through various measures, which can enhance compliance by proactively addressing potential issues. Risk avoidance involves eliminating activities that introduce risks altogether, effectively sidestepping compliance risks. Risk mitigation also seeks to minimize risk impacts through controls or safeguards, thereby reinforcing compliance efforts. Thus, while all these practices focus on managing risk, risk transfer is particularly associated with compliance concerns due to the reliance on external entities to uphold required standards.

8. What is the most appropriate recommendation for a call center that does not assign unique user accounts?

A. Have the current configuration approved by operations management

B. Ensure an audit trail for all existing accounts

C. Implement individual user accounts for all staff

D. Amend the IT policy to allow shared accounts

The most appropriate recommendation is to implement individual user accounts for all staff. This approach enhances security and accountability within the call center environment. Unique user accounts help ensure that each user has their own credentials and access rights, which allows for better tracking of user activities. This is critical in a setting where sensitive customer data may be handled, as it helps maintain both compliance with regulatory requirements and internal policies regarding data security. Unique user accounts also facilitate the enforcement of the principle of least privilege, where employees have access only to the information necessary for their roles, minimizing the risk of unauthorized access to sensitive data. In addition, having individual accounts aids in identifying the responsible party in the event of a breach or security incident, thereby allowing for targeted remedial actions and ensuring that accountability is clearly established. Other recommendations, such as having current configurations approved by management or ensuring an audit trail, do not address the fundamental issue of account management and user accountability. Although these actions may have their benefits, they do not provide the same level of security and operational effectiveness that implementing individual user accounts would achieve. Additionally, amending the IT policy to allow shared accounts would only exacerbate risks related to security and accountability, making it a less desirable option.

9. When a startup is handling software development for an enterprise, what should be recommended to ensure investment protection?

A. Due diligence on the software vendor

B. A quarterly audit of the vendor facilities

C. A source code escrow agreement

D. A high penalty clause in the contract

To ensure investment protection when a startup is developing software for an enterprise, a source code escrow agreement is particularly important. This type of agreement involves depositing the software's source code with a trusted third-party escrow agent. The primary benefit of this arrangement is that it provides security for the enterprise in the event that the vendor is unable or unwilling to support the software in the future, whether due to bankruptcy, business failure, or other unforeseen circumstances. With a source code escrow agreement, the enterprise can access the source code if certain predefined conditions are met, such as the vendor being unable to maintain the software or ceasing operations. This access allows the enterprise to continue using, maintaining, or modifying the software without being entirely dependent on the vendor. Therefore, it gives the enterprise a way to protect its investment in the software development process. In contrast, while conducting due diligence on the software vendor is important, it primarily helps evaluate the vendor's capabilities and risks before engagement, rather than protecting the investment once the software development has begun. A quarterly audit of vendor facilities can serve as a risk management tool, but it does not provide direct investment protection. Similarly, a high penalty clause in the contract may deter non-compliance, but it does not mitigate the risk of losing

10. What should be the primary concern of an IS auditor reviewing external IT service provider management?

A. Minimizing costs for the services provided

B. Evaluating the process for transferring knowledge to the IT department

C. Prohibiting the provider from subcontracting services

D. Determining if the services were provided as contracted

The primary concern of an IS auditor reviewing external IT service provider management should indeed be determining if the services were provided as contracted. This focus is crucial because the main objective of engaging an external service provider is to ensure that they deliver on their defined contractual obligations. Evaluating whether the services meet the agreed-upon standards affects the overall performance, compliance, and satisfaction of the organization. Monitoring compliance with service level agreements (SLAs) not only verifies that the service provider is fulfilling its duties but also safeguards the organization's interests, mitigates risks, and provides assurance regarding the quality and reliability of services received. The auditor's role includes confirming that the service provider's deliverables align with the organization's needs and expectations, as set out in the contract. This alignment is essential for maintaining operational efficiency and managing potential discrepancies between service expectations and actual performance. While minimizing costs, evaluating knowledge transfer processes, and prohibiting subcontracting are important considerations, they do not directly address the primary responsibility of confirming service delivery compliance. These factors can influence overall service quality and cost efficiency but are secondary to ensuring that the contractual requirements are being met effectively.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://cisadomain5.examzify.com

We wish you the very best on your exam journey. You've got this!