

CISA Domain 5 Practice Exam (Sample)

Study Guide



Everything you need from our exam experts!

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright	1
Table of Contents	2
Introduction	3
How to Use This Guide	4
Questions	5
Answers	8
Explanations	10
Next Steps	16

SAMPLE

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

SAMPLE

- 1. What should an IS auditor consider most when reviewing an enterprise's project portfolio?**
 - A. Does not exceed the existing IT budget**
 - B. Is aligned with the investment strategy**
 - C. Has been approved by the IT steering committee**
 - D. Is aligned with the business plan**
- 2. What task is most likely assigned to an IT steering committee within a financial enterprise?**
 - A. Approving IT project plans and budgets**
 - B. Aligning IT to business objectives**
 - C. Advising on IT compliance risk**
 - D. Promoting IT governance practices**
- 3. During a risk management review, what is the critical aspect that an IS auditor should consider?**
 - A. Controls 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**
- 4. What is one major reason for having the IT department involved in cloud application management?**
 - A. To maintain contractual relationships with vendors**
 - B. To ensure compliance with internal IT policies**
 - C. To provide technical support for cloud applications**
 - D. To monitor cloud application performance metrics**
- 5. Why is it important for an organization to conduct periodic risk assessments of their approved software product list?**
 - A. The organization must use the latest versions of software**
 - B. It assists in managing licensing issues**
 - C. Business conditions surrounding vendors may change**
 - D. It ensures that open source software is handled appropriately**

6. What is the first action to take if a key employee leaves with access to sensitive information?

- A. Conduct a security audit**
- B. Notify the compliance officer**
- C. Revoke system access**
- D. Notify the IT department**

7. What is the primary purpose of a decision support system (DSS)?

- A. To solve highly structured problems**
- B. To combine the use of decision models with predetermined criteria**
- C. To make decisions based on data analysis and interactive models**
- D. To support only structured decision-making tasks**

8. When examining a service level agreement for IT outsourcing, what element is most critical for audit purposes?

- A. Completion of service tasks**
- B. Cost-effectiveness analysis**
- C. Independent audit rights**
- D. Client satisfaction measurements**

9. Which aspect should NOT be the primary focus of information security policies?

- A. Procedures for data recovery**
- B. The basis for access control authorization**
- C. Measurement of performance indicators**
- D. Overview of broad security concepts**

10. During an audit, which concern is most troubling if the HR department uses a cloud-based app without proper vendor management?

- A. Maximum acceptable downtime metrics have not been defined**
- B. The IT department does not manage the relationship with the vendor**
- C. The help desk call center is in a different country**
- D. Organization-defined security policies are not applied to the application**

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What should an IS auditor consider most when reviewing an enterprise's project portfolio?

- A. Does not exceed the existing IT budget**
- B. Is aligned with the investment strategy**
- C. Has been approved by the IT steering committee**
- D. Is aligned with the business plan**

When reviewing an enterprise's project portfolio, the most critical aspect to consider is whether the portfolio is aligned with the business plan. This assessment is vital because a project's success largely depends on its relevance and contribution to the broader business objectives and strategies. An alignment with the business plan ensures that the projects undertaken will support the organization's goals and priorities, enabling it to utilize resources effectively and generate maximum value. Projects that align with the business plan are typically positioned to enhance the organization's competitiveness, improve operational efficiency, and drive growth. This alignment is crucial for prioritizing resources, assessing project feasibility and impact, and ensuring that the direction of IT initiatives resonates with the overall mission and vision of the business, ultimately guiding decision-making processes around project execution. While factors such as budget adherence, approval from the IT steering committee, and alignment with the investment strategy are important, they are secondary to the overarching goal of ensuring that the IT projects are strategically integrated into the business's long-term plans. Without this alignment, even well-budgeted and approved projects could fail to deliver meaningful contributions to the enterprise.

2. What task is most likely assigned to an IT steering committee within a financial enterprise?

- A. Approving IT project plans and budgets**
- B. Aligning IT to business objectives**
- C. Advising on IT compliance risk**
- D. Promoting IT governance practices**

The task most commonly assigned to an IT steering committee within a financial enterprise is approving IT project plans and budgets. This committee often plays a pivotal role in overseeing and guiding the direction of IT initiatives, ensuring that projects align with the broader strategic goals of the organization. By approving project plans and budgets, the steering committee ensures resources are allocated appropriately and that IT initiatives are not only feasible but also provide value to the organization. Given the financial context, this oversight helps mitigate risks associated with IT investments and ensures that the projects undertaken support the overall mission and objectives of the financial enterprise. While aligning IT to business objectives, advising on IT compliance risk, and promoting IT governance practices are also important functions within an organization, the steering committee's primary responsibility is typically centered around the tactical and strategic validation of IT projects and the allocation of funds to support those initiatives. This ensures that IT spending is justified and aligned with the financial enterprise's priorities.

3. During a risk management review, what is the critical aspect that an IS auditor should consider?

- A. Controls 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 critical aspect of presenting IT risk in business terms is essential for ensuring that stakeholders understand the implications of those risks on the organization's overall goals and objectives. When risks are articulated in a language and context that resonate with business leaders, it facilitates informed decision-making and prioritization of risk management efforts. This approach helps to bridge the gap between technical jargon and business strategy, enabling leadership to allocate resources effectively and align risk management with organizational priorities. By framing IT risks in business terms, an IS auditor can emphasize how these risks can impact financial performance, brand reputation, operational efficiency, and regulatory compliance. This perspective not only highlights the significance of the risks but also helps foster a culture of risk awareness throughout the organization, making it easier to gain support for risk mitigation initiatives. In contrast, while controls based on cost-benefit analysis, adherence to global standards in the risk management framework, and the existence of an approval process for risk response are important elements, they do not directly address the need for effective communication and understanding among stakeholders. Without context and clarity in how IT risks affect the business, the impact of those risks may be underestimated or ignored entirely, leading to inadequate risk responses.

4. What is one major reason for having the IT department involved in cloud application management?

- A. To maintain contractual relationships with vendors**
- B. To ensure compliance with internal IT policies**
- C. To provide technical support for cloud applications**
- D. To monitor cloud application performance metrics**

Having the IT department involved in cloud application management is crucial for ensuring compliance with internal IT policies. This involvement helps ensure that the cloud applications adhere to established protocols regarding data security, privacy, risk management, and overall governance. Internal policies often dictate how data is handled, who has access, and what security measures must be employed. By having IT engaged in the management of these applications, organizations can better ensure that all cloud services used are vetted, aligned with business objectives, and compliant with both internal standards and external regulations. This oversight plays a vital role in mitigating potential risks that may arise from the use of cloud technologies, which may otherwise introduce challenges like unauthorized data access or violations of data protection laws. While other factors such as maintaining vendor relationships, providing technical support, and monitoring performance metrics are certainly important aspects of cloud management, they do not directly address the critical need for compliance with internal policies. Ensuring that cloud applications align with established IT governance frameworks is foundational to protecting organizational assets and data integrity.

5. Why is it important for an organization to conduct periodic risk assessments of their approved software product list?

- A. The organization must use the latest versions of software**
- B. It assists in managing licensing issues**
- C. Business conditions surrounding vendors may change**
- D. It ensures that open source software is handled appropriately**

Conducting periodic risk assessments of an organization's approved software product list is crucial because business conditions surrounding vendors may change over time. This assessment helps identify potential risks related to the software products being used, which could be influenced by changes in vendor stability, reputation, compliance with regulations, or market conditions. For instance, a vendor may face financial difficulties leading to reduced support for their software, or they might introduce new terms of service that could expose the organization to legal or compliance risks. By regularly evaluating these aspects, the organization can proactively address any emerging risks, ensuring that their software remains secure, compliant, and supportive of business operations. This vigilance is essential for maintaining a robust risk management strategy, thereby protecting the organization from potential disruptions or vulnerabilities associated with the software it relies on.

6. What is the first action to take if a key employee leaves with access to sensitive information?

- A. Conduct a security audit**
- B. Notify the compliance officer**
- C. Revoke system access**
- D. Notify the IT department**

The first action to take when a key employee leaves with access to sensitive information is to revoke system access. This is crucial because it ensures that the departing individual can no longer access confidential or sensitive data, thereby protecting the organization from potential data breaches or unauthorized information disclosure. This step is pivotal since the immediate priority is to secure the organization's information assets and prevent any misuse by the exiting employee. Revoking system access promptly minimizes any risks associated with lingering access rights, which could lead to data theft or loss. While conducting a security audit, notifying a compliance officer, or informing the IT department are all important steps in the overall process of managing the situation effectively, revoking access is the most urgent action. It directly addresses the potential threat posed by the employee's departure, ensuring that security is tightened immediately.

7. What is the primary purpose of a decision support system (DSS)?

- A. To solve highly structured problems**
- B. To combine the use of decision models with predetermined criteria**
- C. To make decisions based on data analysis and interactive models**
- D. To support only structured decision-making tasks**

The primary purpose of a decision support system (DSS) is to aid in making decisions based on data analysis and interactive models. A DSS is designed to provide comprehensive, interactive facilities that help users utilize data and models to solve complex problems, enabling them to make informed and effective decisions. This system integrates various data sources and applies advanced analytical techniques, allowing users to manipulate and examine scenarios interactively, ultimately leading to improved decision-making outcomes. The focus on data analysis emphasizes the ability of the DSS to process and analyze large volumes of data, which is crucial when making choices in uncertain or complex environments. Additionally, the interactive models allow decision-makers to simulate different scenarios and outcomes, fostering a better understanding of the consequences of their choices and enabling dynamic adjustments to various factors involved in the decision-making process. This makes the DSS a powerful tool for addressing challenges that may not have a straightforward or structured solution.

8. When examining a service level agreement for IT outsourcing, what element is most critical for audit purposes?

- A. Completion of service tasks**
- B. Cost-effectiveness analysis**
- C. Independent audit rights**
- D. Client satisfaction measurements**

The element most critical for audit purposes in a service level agreement (SLA) for IT outsourcing is independent audit rights. This aspect enables the organization to have a structured approach to verify that the service provider is meeting the agreed-upon terms and conditions of the SLA. Independent audit rights ensure that there is an unbiased party that can assess compliance with service levels, performance metrics, and quality standards outlined in the agreement. These audit rights facilitate transparency and accountability, allowing the organization to confirm that the service provider is adhering to the performance metrics stipulated in the SLA. While an entity can conduct or arrange for independent audits, it not only fosters trust but also provides a mechanism for addressing any discrepancies or breaches in service delivery, ultimately serving to protect the interests of both parties involved in the outsourcing agreement. While completion of service tasks, cost-effectiveness analysis, and client satisfaction measurements are important aspects of an SLA and contribute to overall service quality and performance, they do not provide the essential independent verification process that audit rights offer. The ability to perform independent audits plays a crucial role in maintaining oversight and ensuring adherence to the contractual obligations, making it the most critical element for audit purposes.

9. Which aspect should NOT be the primary focus of information security policies?

- A. Procedures for data recovery**
- B. The basis for access control authorization**
- C. Measurement of performance indicators**
- D. Overview of broad security concepts**

The primary focus of information security policies is to establish the framework and principles that guide the organization in protecting its information assets. While all the aspects listed are important elements of a comprehensive security program, focusing on the measurement of performance indicators as the primary aspect may not align with the fundamental purpose of security policies. Information security policies are designed to provide an overview of broad security concepts, outline procedures for protecting data (like recovery processes), and set the foundation for access control measures that ensure only authorized users have access to sensitive information. These elements directly relate to the strategic direction and operational requirements of information security.

Conversely, while performance indicators are vital for assessing the effectiveness of security measures and for continuous improvement, they should stem from the established policies rather than being the primary focus of the policies themselves. The policies serve to create a holistic approach to security, and while performance measurement is necessary, it is more of a byproduct—a means of evaluating the effectiveness of the policies rather than a central focus of what the policies themselves should entail.

10. During an audit, which concern is most troubling if the HR department uses a cloud-based app without proper vendor management?

- A. Maximum acceptable downtime metrics have not been defined**
- B. The IT department does not manage the relationship with the vendor**
- C. The help desk call center is in a different country**
- D. Organization-defined security policies are not applied to the application**

The most troubling concern when an HR department uses a cloud-based application without proper vendor management is that organization-defined security policies are not applied to the application. This situation poses significant risks as it means that the application may not be adhering to the organization's established protocols for data protection, confidentiality, integrity, and compliance with regulations. When security policies are not enforced, sensitive employee data managed by the HR department is at increased risk of unauthorized access, breaches, or misuse. Lack of adherence to these security policies can lead to vulnerabilities in the application that cyber threats could exploit, potentially resulting in data leaks or compliance violations that can have serious legal and financial repercussions for the organization. While the other concerns listed—such as maximum acceptable downtime metrics, vendor relationship management, and the location of the help desk—are important in ensuring the overall resilience and effectiveness of the service, the primary concern with security policies directly impacts the organization's ability to protect its sensitive information and maintain trust with employees.

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!

SAMPLE