CISA DOMAIN 2 PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cisadomain2.examzify.com

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. What does a lack of adequate security controls define?

A. Threat

B. Asset

C. Impact

D. Vulnerability

2. Why is it essential to have a software escrow agreement with a vendor?

A. To ensure compliance with higher management

B. To retain access to source code if the vendor goes out of business

C. To facilitate a smooth contract renegotiation

D. To standardize software usage across departments

3. When reviewing an organization's approved software product list, what should be the most important verification?

A. The risk associated with the use of products is periodically assessed

B. The latest version of software is listed for each product

C. The list does not contain open source software due to licensing issues

D. After-hours support is offered

4. During which phase of e-business security assessment should risks first be identified?

A. After vulnerabilities are documented

B. Before detailed solution development

C. While checking budget alignments

D. After confirming software functionality

5. In reviewing a business process reengineering effort, what is the primary concern?

A. Elimination of controls during reengineering

B. Inadequate resources for support

C. Lack of audit involvement in the process

D. Employees with limited process knowledge

SAMPLE

6. What is essential for an effective IT strategy within an organization?

A. Alignment with evolving market trends

B. Focus on the latest technologies

C. Alignment with the business strategy

D. Strict adherence to regulatory requirements

7. 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

8. What is the most critical success factor when developing a formal enterprise security program?

A. Establishment of a review board

B. Creation of a security unit

C. Effective support of an executive sponsor

D. Selection of a security process owner

9. What measure is best for prioritizing IT projects based on overall investment performance?

A. Risk self-assessment completion

B. Conducting IS audits

C. Analysis of investment portfolios

D. Performing risk assessments

10. To best align an IT project portfolio with organizational priorities, what should an IS auditor recommend?

A. Define a balanced scorecard for performance measurement

B. Consider user satisfaction in performance indicators

C. Select projects based on business benefits and risk

D. Modify the yearly portfolio definition process

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does a lack of adequate security controls define?

A. Threat

B. Asset

C. Impact

D. Vulnerability

A lack of adequate security controls defines a vulnerability. Vulnerabilities are weaknesses in a system, application, or organization that can be exploited by threats to gain unauthorized access or cause harm. They arise from inadequate security measures, such as insufficient firewalls, weak authentication mechanisms, or poor data handling practices. When security controls are not implemented effectively, they create openings for potential attacks, allowing threats to exploit these vulnerabilities. Understanding vulnerabilities is crucial in the field of cybersecurity, as it helps organizations identify areas that need improvement to enhance their overall security posture. By addressing vulnerabilities through targeted security controls, organizations can mitigate risks and protect their assets more effectively.

2. Why is it essential to have a software escrow agreement with a vendor?

A. To ensure compliance with higher management

B. To retain access to source code if the vendor goes out of business

C. To facilitate a smooth contract renegotiation

D. To standardize software usage across departments

Having a software escrow agreement with a vendor is crucial primarily to ensure access to the source code if the vendor goes out of business or fails to meet their obligations. This agreement involves placing the software's source code, along with relevant documentation, into a neutral third-party escrow service. This arrangement protects the client by ensuring they have the necessary resources to maintain and modify the software independently if the vendor can no longer provide support or the software is no longer available. Access to the source code is essential for the longevity and sustainability of the software application, especially in cases where critical systems depend on that software. If a vendor ceases operations or is unable to provide necessary updates or support, having the source code allows the organization to continue using the software without interruption. This aspect is particularly important for businesses that rely on specific applications to operate efficiently and effectively. Consequently, the other options do not capture the primary purpose and benefit of a software escrow agreement as accurately as the correct choice. While compliance, contract renegotiation, and standardization can be important in the context of vendor relationships, they are not the main focus or unique advantage provided by a software escrow agreement.

SAMPLE

3. When reviewing an organization's approved software product list, what should be the most important verification?

A. The risk associated with the use of products is periodically assessed

B. The latest version of software is listed for each product

C. The list does not contain open source software due to licensing issues

D. After-hours support is offered

The most important verification when reviewing an organization's approved software product list is the periodic assessment of the risks associated with the use of these products. This is crucial because even approved software can introduce vulnerabilities or become obsolete due to the rapid changes in technology, security threats, and compliance requirements. By regularly assessing risks, the organization can ensure that it remains aware of potential security threats and can take proactive measures to mitigate those risks, thereby protecting its data and systems. While identifying the latest version of the software is important for maintaining security and functionality, and ensuring no open source software is included may address potential legal issues, these factors are secondary to the overarching need for ongoing risk management. Similarly, after-hours support is valuable but does not directly contribute to the overall security posture of the organization. Prioritizing risk assessment ensures that the organization's software environment continues to meet security and operational requirements over time.

4. During which phase of e-business security assessment should risks first be identified?

A. After vulnerabilities are documented

B. Before detailed solution development

C. While checking budget alignments

D. After confirming software functionality

The phase during which risks should first be identified is before detailed solution development. In any security assessment process, understanding and identifying risks is a foundational step that guides the decision-making and prioritization of security measures. This assessment serves to identify potential threats and vulnerabilities associated with the e-business environment. Identifying risks early allows organizations to take a proactive approach to security, ensuring that potential issues are considered when developing solutions. By recognizing risks beforehand, organizations can design more effective security controls, allocate resources appropriately, and ultimately reduce the likelihood of security incidents. The other options focus on activities that take place after risks have been identified, which would not allow for an effective preemptive strategy. Documenting vulnerabilities, checking budgets, or confirming software functionality are critical tasks but hinge on an initial assessment of risks to be effective and relevant.

SAMPLE

5. In reviewing a business process reengineering effort, what is the primary concern?

A. Elimination of controls during reengineering

B. Inadequate resources for support

C. Lack of audit involvement in the process

D. Employees with limited process knowledge

The primary concern in a business process reengineering effort revolves around the elimination of controls during the reengineering process. Business process reengineering is fundamentally about redesigning existing processes to achieve significant improvements in performance metrics such as cost, quality, and speed. However, in the zeal to streamline operations and eliminate inefficiencies, there's a risk of dropping critical controls that ensure the integrity, compliance, and security of those processes. Controls are essential for managing risks and providing assurance that the processes perform as intended. Without these controls, the organization may expose itself to operational risks, compliance issues, and potential fraud, which can ultimately undermine the benefits intended from reengineering initiatives. Therefore, maintaining or appropriately redesigning controls during such efforts is crucial to ensure that while processes become more efficient, they do not lose their effectiveness in governance and risk management. This concern stands out as a priority because the success of reengineering is not just measured by improved performance but also by the sustainability and security of the newly designed processes. It is therefore critical to carefully assess how controls can be integrated or adapted within the newly defined processes rather than simply removed in the name of efficiency.

6. What is essential for an effective IT strategy within an organization?

A. Alignment with evolving market trends

B. Focus on the latest technologies

C. Alignment with the business strategy

D. Strict adherence to regulatory requirements

An effective IT strategy is fundamentally about ensuring that IT initiatives and investments are closely linked to the overall goals and objectives of the organization. Alignment with the business strategy ensures that the IT function supports and enhances the business's capabilities, improves operational efficiency, and facilitates the achievement of business outcomes. When IT aligns well with the business strategy, it allows for better prioritization of technology investments, ensures that resources are utilized effectively, and encourages collaboration between IT and other business units. This is crucial in responding to market changes and leveraging technology for competitive advantage. While alignment with evolving market trends, focus on the latest technologies, and adherence to regulatory requirements are important considerations, they should be secondary to ensuring that the IT strategy supports the business strategy. For instance, adopting the latest technologies may not yield beneficial outcomes if they do not align with the organization's strategic goals or market needs. Similarly, while compliance is essential from a legal standpoint, it should also fit into the broader strategic framework. Therefore, the most critical aspect of an effective IT strategy lies in its alignment with the business strategy.

SAMPLE

7. 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.

8. What is the most critical success factor when developing a formal enterprise security program?

A. Establishment of a review board

B. Creation of a security unit

C. Effective support of an executive sponsor

D. Selection of a security process owner

The most critical success factor when developing a formal enterprise security program is the effective support of an executive sponsor. This role is paramount because executive sponsors provide the necessary backing at the highest levels of the organization, ensuring that security initiatives have the authority, resources, and visibility they require to be successful. Their commitment can help to align security objectives with business goals, fostering a culture of security awareness throughout the organization. Additionally, executive sponsors can facilitate cross-departmental collaboration, ensure that security policies are adhered to, and promote investment in security resources. Their support also aids in communicating the importance of security measures to all stakeholders, making it easier to garner buy-in from employees at all levels. In contrast, while establishing a review board, creating a security unit, and selecting a security process owner are certainly important components of a security program, their effectiveness and functionality are heavily reliant on the commitment and influence of an executive sponsor. Without such sponsorship, even the best-designed security processes and teams may struggle to implement policies effectively or secure the necessary resources and training needed to operate successfully.

SAMPLE

9. What measure is best for prioritizing IT projects based on overall investment performance?

A. Risk self-assessment completion

B. Conducting IS audits

C. Analysis of investment portfolios

D. Performing risk assessments

The most effective measure for prioritizing IT projects based on overall investment performance is the analysis of investment portfolios. This approach allows organizations to evaluate the potential returns of various IT projects in relation to the investments required for each. By assessing the performance of these projects as part of a larger investment portfolio, decision-makers can identify which initiatives will yield the best financial outcomes, optimize resource allocation, and ultimately enhance the organization's return on investment (ROI). Analyzing investment portfolios involves consideration of factors such as risk, profitability, alignment with strategic goals, and market trends, enabling a comprehensive view of how each project contributes to the organization's financial performance. This method helps prioritize projects that not only meet business objectives but also demonstrate the best potential for generating value. In contrast, the other options, while important for governance and compliance, do not directly measure investment performance in the same way. Risk self-assessment completion and performing risk assessments focus on identifying and managing potential risks but do not provide a clear picture of financial returns. Conducting IS audits can offer insights into the effectiveness and compliance of IT projects but is not primarily concerned with prioritizing projects based on their investment performance. Thus, analyzing investment portfolios stands out as the best measure for this specific purpose.

10. To best align an IT project portfolio with organizational priorities, what should an IS auditor recommend?

A. Define a balanced scorecard for performance measurement

B. Consider user satisfaction in performance indicators

C. Select projects based on business benefits and risk

D. Modify the yearly portfolio definition process

Selecting projects based on business benefits and risk is the most effective strategy for aligning an IT project portfolio with organizational priorities. This approach ensures that resources are allocated to projects that not only support the organization's strategic goals but also provide the highest potential returns while managing risk effectively. When projects are evaluated based on their business benefits, decision-makers can prioritize initiatives that deliver tangible value, such as increased revenue, cost savings, or enhanced service delivery. Additionally, incorporating risk assessment into this selection process allows for a more comprehensive understanding of potential challenges and impacts associated with each project. By considering both the benefits and risks, organizations can make informed decisions that effectively align the IT project portfolio with the broader organizational objectives and priorities. This methodology fosters a more strategic approach to project management, ensuring that the chosen projects not only fit within the current organizational framework but also contribute positively to the organization's overall mission and vision.

SAMPLE

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://cisadomain2.examzify.com

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

SAMPLE