CISSP DOMAIN 7 COMPLIANCE MAINTENANCE PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cisspdom7.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 is a compliance gap analysis?

A. A process for identifying discrepancies between current practices and compliance requirements

B. A technique for assessing organizational resources

C. A method for training compliance staff

D. A checklist for compliance audits

2. Which document commonly outlines an organization's commitment to compliance?

A. Business continuity plan

B. Compliance policy or compliance management plan

C. Employee handbook

D. Annual report

3. How can risk management assist compliance programs?

A. By identifying only financial risks

B. By implementing additional regulations

C. By informing decisions to mitigate compliance risks

D. By reducing workforce size

4. The process of assessing risks and developing security plans is part of which authorization activity?

A. Change management

B. Risk assessment

C. Compliance auditing

D. Performance evaluation

5. What characterizes a formal assessment?

A. It occurs continually and is informal in nature

B. It is a discrete event with specified goals

C. It is based solely on user feedback

D. It does not require documentation

SAMPLE

6. What is the main purpose of vulnerability scanning?

A. To improve system performance

B. To provide user training

C. To identify outdated or vulnerable software

D. To map user behavior on the system

7. Which of the following is a key element of a configuration management plan?

A. Employee performance reviews

B. Implementation details for changes

C. Customer service procedures

D. Product marketing strategies

8. What typically triggers the need for regulatory change management?

A. Employee turnover

B. Changes in regulations affecting the organization

C. Technological advancements

D. Market competition

9. What is the purpose of ISO/IEC 38500?

A. To provide IT governance guidelines

B. To establish auditing processes

C. To protect personal information

D. To improve quality management systems

10. What do policies in a system typically govern?

A. Internet usage

B. System operation, management, and maintenance

C. Employee hiring practices

D. Training and development

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is a compliance gap analysis?

A. A process for identifying discrepancies between current practices and compliance requirements

B. A technique for assessing organizational resources

C. A method for training compliance staff

D. A checklist for compliance audits

A compliance gap analysis is fundamentally a process aimed at identifying discrepancies between an organization's current practices and the applicable compliance requirements. This involves reviewing existing policies, procedures, and controls to determine whether they meet the standards set forth by relevant laws, regulations, and industry standards. The importance of this analysis lies in its ability to reveal vulnerabilities or areas of non-compliance that need to be addressed to mitigate risks and ensure that the organization is operating within legal and regulatory frameworks. By understanding where these gaps exist, organizations can develop action plans to enhance compliance, improve practices, and reduce the likelihood of non-compliance penalties. This process is essential for maintaining compliance and building a robust compliance framework, allowing the organization to adapt to changing regulations effectively. It sets the foundation for further compliance initiatives and ensures that organizational practices align with external requirements, thereby strengthening the overall governance of the organization.

2. Which document commonly outlines an organization's commitment to compliance?

A. Business continuity plan

B. Compliance policy or compliance management plan

C. Employee handbook

D. Annual report

The compliance policy or compliance management plan serves as a foundational document that articulates an organization's commitment to adhering to relevant laws, regulations, standards, and internal policies. This document typically outlines the framework for compliance management within the organization, detailing responsibilities, processes, and measures in place to ensure compliance is maintained. Organizations use this document to establish the tone for compliance and governance, demonstrating to stakeholders including employees, customers, and regulatory bodies that they prioritize compliance throughout their operations. It also provides guidelines on how to identify, assess, and mitigate compliance risks, ensuring that everyone in the organization understands their role in upholding compliance standards. While a business continuity plan focuses more on maintaining critical business functions during a crisis, and an employee handbook provides guidelines for employees regarding workplace policies and practices, the compliance policy specifically addresses compliance-related issues. An annual report typically summarizes an organization's performance and financial status rather than its compliance commitments. Thus, the compliance policy or compliance management plan is the most appropriate document to outline an organization's commitment to compliance.

SAMPLE

3. How can risk management assist compliance programs?

A. By identifying only financial risks

B. By implementing additional regulations

C. By informing decisions to mitigate compliance risks

D. By reducing workforce size

Risk management plays a crucial role in enhancing compliance programs by informing decisions that aim to mitigate compliance risks. This process involves systematically identifying, assessing, and prioritizing risks associated with regulatory requirements. By understanding these risks, organizations can implement effective strategies to minimize the likelihood of non-compliance and its associated penalties, which not only protects the organization but also promotes a culture of compliance. Furthermore, this proactive approach enables organizations to allocate resources efficiently, ensuring that they focus on the most significant compliance threats. By integrating risk management into compliance efforts, organizations can effectively adapt their policies and practices as regulations evolve, creating a more resilient compliance framework. The other options do not align with the core function of risk management in relation to compliance. Identifying only financial risks overlooks broader compliance issues, implementing additional regulations does not inherently address existing risks, and reducing workforce size does not contribute positively to managing compliance-related risks. Instead, it can create gaps in compliance oversight and awareness.

4. The process of assessing risks and developing security plans is part of which authorization activity?

A. Change management

B. Risk assessment

C. Compliance auditing

D. Performance evaluation

The process of assessing risks and developing security plans aligns directly with risk assessment activities. This is a critical component of the risk management framework, where an organization identifies potential threats and vulnerabilities to its assets, evaluates the risks associated with them, and formulates strategies to mitigate these risks. By conducting a thorough risk assessment, organizations can prioritize where to allocate resources and how to best protect their information assets and systems. The development of security plans as a result of the assessment ensures that the organization addresses identified vulnerabilities and implements necessary controls. This proactive approach not only helps in compliance with regulatory requirements but also establishes a foundation for ongoing security practices. In contrast, change management focuses more on how changes to configurations, processes, or systems are controlled to minimize disruption and maintain service quality rather than on assessing risks. Compliance auditing involves verifying adherence to policies, regulations, and standards after controls are implemented. Performance evaluation is about assessing the effectiveness and efficiency of security measures already in place, rather than the initial assessment and planning phase of security management. Thus, the emphasis on risk evaluation and strategic development distinctly categorizes this activity under risk assessment.

SAMPLE

5. What characterizes a formal assessment?

A. It occurs continually and is informal in nature

B. It is a discrete event with specified goals

C. It is based solely on user feedback

D. It does not require documentation

A formal assessment is characterized by being a discrete event with specified goals. This means that a formal assessment is planned and structured, focusing on achieving clear objectives. It is typically conducted at specific intervals or milestones, enabling organizations to evaluate compliance with established standards, policies, or regulations. The structured approach ensures that the assessment results are consistent and repeatable, allowing for meaningful comparisons and analyses over time. Furthermore, formal assessments usually involve predefined criteria and methodologies that guide the evaluation process, which may include audits, risk assessments, or compliance checks. Such assessments yield documented findings that can be used to inform decision-making and drive improvements. The emphasis on documentation and goal orientation distinguishes formal assessments from informal or ongoing evaluations, which may lack the rigor associated with a structured approach.

6. What is the main purpose of vulnerability scanning?

A. To improve system performance

B. To provide user training

C. To identify outdated or vulnerable software

D. To map user behavior on the system

The main purpose of vulnerability scanning is to identify outdated or vulnerable software within a system. This process involves examining the networked devices, applications, and systems to uncover security weaknesses that could be exploited by attackers. By pinpointing these vulnerabilities, organizations can take proactive measures to mitigate risks, apply security patches, and implement additional controls to enhance their security posture. Vulnerability scanning plays a critical role in an organization's overall security strategy, as it helps maintain compliance with various regulatory frameworks. Regular scans ensure that software is kept up to date and that any known vulnerabilities are addressed promptly, thereby minimizing the potential attack surface and protecting sensitive data. Other potential functions related to system performance, user training, and user behavior mapping do not align with the primary goal of vulnerability scanning, which is strictly focused on identifying and addressing security weaknesses.

SAMPLE

7. Which of the following is a key element of a configuration management plan?

A. Employee performance reviews

B. Implementation details for changes

C. Customer service procedures

D. Product marketing strategies

A configuration management plan is focused on ensuring that an organization's systems and software are consistently controlled and monitored throughout their lifecycle. One of the key elements of such a plan is the implementation details for changes. This includes defining how changes to the system will be proposed, evaluated, approved, and documented. By having clear procedures for implementing changes, organizations can maintain the integrity, security, and performance of their systems. This element aligns with the objectives of configuration management to establish baselines, track changes, and enforce policies that govern the system's configuration. While the other options touch upon different areas of organizational operations, they do not pertain directly to the core focus of a configuration management plan. Employee performance reviews, for example, relate more to human resources and personnel management, customer service procedures are about operational support and user engagement, and product marketing strategies focus on how products are presented to the market. These aspects, while important in their own right, do not contribute to the structured management of configuration processes, which is essential for the effective governance of IT assets.

8. What typically triggers the need for regulatory change management?

A. Employee turnover

B. Changes in regulations affecting the organization

C. Technological advancements

D. Market competition

The need for regulatory change management is primarily triggered by changes in the regulations that affect the organization. Regulatory environments are dynamic, and laws or guidelines can evolve due to various factors, such as new legislation, shifts in public policy, or responses to socio-economic events. Organizations must adapt to these changes to ensure compliance and avoid potential penalties or legal issues. When regulations change, it can impact a wide range of business operations, including data protection, financial reporting, health and safety standards, and more. This necessitates updates to policies, procedures, and practices within the organization to align with the new requirements. Therefore, effective change management processes are crucial for keeping the organization informed and compliant with the current legal landscape. While employee turnover, technological advancements, and market competition can all influence organizational operations and may lead to change, they are not direct triggers for regulatory change management like changes in regulations are. Instead, they may require adjustments in strategy or operational procedures rather than a direct response to compliance requirements.

SAMPLE

9. What is the purpose of ISO/IEC 38500?

A. To provide IT governance guidelines

B. To establish auditing processes

C. To protect personal information

D. To improve quality management systems

The purpose of ISO/IEC 38500 is to provide guidelines for the governance of information technology (IT) within organizations. It is aimed at assisting top management in understanding the importance of effective governance of IT, ensuring that IT supports and enhances the organization's objectives and strategies. This standard lays out principles and a framework for making decisions related to IT, emphasizing accountability, strategic alignment, risk management, resource management, and performance measurement. The guidelines are designed to be applicable to any organization, regardless of size or type, making them versatile for various governance contexts. They help ensure that organizations can make informed decisions regarding IT investments, ensuring compliance with relevant laws and regulations while maximizing value from IT resources. Other options do not align with the intent of ISO/IEC 38500. Auditing processes, for instance, are typically covered by different ISO standards that focus on compliance checks rather than governance itself. Protecting personal information would fall under different frameworks that specifically address data protection and privacy, while quality management systems are governed by other regulations and standards focused on operational processes and improvement specific to quality. Therefore, option A correctly describes the scope and intent of ISO/IEC 38500.

10. What do policies in a system typically govern?

A. Internet usage

B. System operation, management, and maintenance

C. Employee hiring practices

D. Training and development

Policies in a system primarily govern system operation, management, and maintenance because they provide a structured framework that dictates how the system should function, how it should be managed, and what maintenance procedures must be followed. These policies ensure consistency, security, and compliance with regulations. They typically outline responsibilities, procedures, and controls necessary to ensure the proper and secure operation of information systems. While other areas like internet usage, employee hiring practices, and training and development are important aspects of an organization's overall governance, they do not specifically pertain to the policies governing the intricate details of system operation and maintenance. Such focused policies are critical for organizations to manage technical environments efficiently and securely, ensuring that systems operate smoothly while adhering to relevant regulatory and compliance requirements.

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://cisspdom7.examzify.com

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

SAMPLE