

# CISSP Domain 7 Compliance Maintenance Practice Test (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 is the purpose of a code of conduct in compliance?**
  - A. To establish a clear set of expectations for ethical behavior and compliance with regulations**
  - B. To provide detailed procedures for compliance audits**
  - C. To offer training modules for employees**
  - D. To document compliance technology used within the organization**
  
- 2. How does vulnerability scanning contribute to overall system maintenance?**
  - A. By reducing the likelihood of system downtime**
  - B. By providing insights into user behavior patterns**
  - C. By facilitating enhancements in user interfaces**
  - D. By ensuring all software is visually appealing**
  
- 3. Usability testing helps to inform what kind of system improvements?**
  - A. Visual aesthetic enhancements**
  - B. Technological upgrades only**
  - C. User experience and functionality enhancements**
  - D. Database optimization strategies**
  
- 4. 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**
  
- 5. What is one key benefit of user feedback gathered during usability testing?**
  - A. Identification of additional software licenses needed**
  - B. Improvement of product marketing strategies**
  - C. Enhancing system features aligned with user preferences**
  - D. Determining cost of system upgrades**

- 6. What is the primary purpose of logs in a system?**
- A. To provide user documentation**
  - B. To document events and activities of the system**
  - C. To analyze performance metrics**
  - D. To secure user data**
- 7. ISO 31000 offers guidance primarily on which topic?**
- A. Quality management**
  - B. Risk management**
  - C. Information security**
  - D. Software maintenance**
- 8. What is the impact of non-compliance on an organization's reputation?**
- A. Increased customer loyalty**
  - B. Improved media relations**
  - C. Loss of trust and customer attrition**
  - D. Growth in market share**
- 9. How does risk management integrate with compliance efforts?**
- A. By avoiding any connection between the two**
  - B. By helping to identify risks that could impact compliance**
  - C. By solely focusing on financial risks**
  - D. By providing legal representation**
- 10. ISO/IEC 27001 specifies requirements for which of the following?**
- A. Data encryption**
  - B. Information security management**
  - C. Software testing**
  - D. Environmental management**

## Answers

SAMPLE

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

SAMPLE

## **Explanations**

SAMPLE

## 1. What is the purpose of a code of conduct in compliance?

- A. To establish a clear set of expectations for ethical behavior and compliance with regulations**
- B. To provide detailed procedures for compliance audits**
- C. To offer training modules for employees**
- D. To document compliance technology used within the organization**

The purpose of a code of conduct in compliance is primarily to establish a clear set of expectations for ethical behavior and adherence to regulations. A well-crafted code of conduct serves as a framework for how employees should act in various situations, helping to promote a culture of integrity and respect within the organization. It guides employees on the principles of professional conduct that align with the company's values and compliance with relevant laws. This foundational aspect is critical, as it enables organizations to reinforce a commitment to ethical standards and compliance obligations, effectively minimizing the risk of misconduct or non-compliance. While providing detailed procedures for compliance audits, offering training modules for employees, and documenting compliance technology are important aspects of a compliance program, they are not the primary function of a code of conduct. A code of conduct specifically focuses on setting ethical and behavioral standards rather than detailed procedures, training materials, or technology documentation. This makes it an essential element of an organization's broader compliance strategy.

## 2. How does vulnerability scanning contribute to overall system maintenance?

- A. By reducing the likelihood of system downtime**
- B. By providing insights into user behavior patterns**
- C. By facilitating enhancements in user interfaces**
- D. By ensuring all software is visually appealing**

Vulnerability scanning plays a crucial role in overall system maintenance by proactively identifying security weaknesses within systems and applications. By detecting vulnerabilities before they can be exploited by attackers, organizations can implement appropriate measures, such as patches or configuration changes, thus reducing the likelihood of system downtime caused by security incidents. This functionality helps maintain the integrity and availability of systems, ensuring that they operate smoothly and securely. While understanding user behavior patterns, enhancing user interfaces, and focusing on visual appeal are important aspects of system design and user experience, they do not directly relate to the fundamental purpose of vulnerability scanning, which is to identify and mitigate risks to system reliability and security. Therefore, emphasizing the role of vulnerability scanning in maintaining system uptime and reducing potential disruptions underscores its importance in the broader context of system maintenance.

### 3. Usability testing helps to inform what kind of system improvements?

- A. Visual aesthetic enhancements
- B. Technological upgrades only
- C. User experience and functionality enhancements**
- D. Database optimization strategies

Usability testing plays a crucial role in enhancing user experience and functionality within a system. By observing how real users interact with a product, stakeholders can identify pain points and areas of confusion. This feedback leads to improvements that make the interface more intuitive, efficient, and user-friendly, directly impacting overall user satisfaction and engagement. The insights gathered from usability testing can reveal issues related to navigation, readability, and task completion rates. Enhancements driven by these findings may involve simplifying workflows, better organizing information, or adjusting the design to align with user expectations. In contrast, while options such as visual aesthetic enhancements, technological upgrades, and database optimization may also be important, they do not primarily stem from the insights gained through usability testing. Usability testing focuses more on how users experience and interact with the system rather than solely on technology or aesthetic aspects. Therefore, the answer highlights the core purpose of usability testing in improving user interaction and functionality.

### 4. 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.

**5. What is one key benefit of user feedback gathered during usability testing?**

- A. Identification of additional software licenses needed**
- B. Improvement of product marketing strategies**
- C. Enhancing system features aligned with user preferences**
- D. Determining cost of system upgrades**

The key benefit of user feedback gathered during usability testing is that it significantly enhances system features in alignment with user preferences. This process allows developers and designers to understand how real users interact with the system, revealing specific areas where the user experience can be improved. By gathering feedback directly from users, organizations can better identify which features are valuable, intuitive, or needed, leading to more effective enhancements in both the usability and functionality of the product. This user-centered approach ensures that developments are not only technically sound but also aligned with what users actually want and need, ultimately leading to higher satisfaction and engagement with the system.

**6. What is the primary purpose of logs in a system?**

- A. To provide user documentation**
- B. To document events and activities of the system**
- C. To analyze performance metrics**
- D. To secure user data**

The primary purpose of logs in a system is to document events and activities of the system. Logs serve as a historical record that captures a wide range of information regarding system operations, user activities, and security events. This documentation plays a critical role in monitoring system health, diagnosing issues, and investigating incidents when they arise. By maintaining detailed logs, organizations can track which actions were taken by users or systems at specific times, providing valuable insights for audits, compliance reporting, and incident response efforts. These logs help security professionals to identify unauthorized access attempts, system failures, and other events that could impact the integrity and availability of the system. While performance metrics, user data security, and user documentation are important aspects of system management, the fundamental role of logging is to create a comprehensive record of system activities which facilitates better management and security oversight.

## 7. ISO 31000 offers guidance primarily on which topic?

- A. Quality management
- B. Risk management**
- C. Information security
- D. Software maintenance

ISO 31000 provides a comprehensive framework for effective risk management. Its primary focus is on helping organizations understand and manage risks to achieve their objectives. This standard outlines the principles and guidelines for creating a risk management framework and process, ensuring that risks are identified, assessed, communicated, and monitored effectively. The guidance of ISO 31000 is applicable across various sectors and industries, making it a versatile tool for integrating risk management into strategic decision-making. It emphasizes the importance of customizing risk management practices to fit the organizational context, culture, and stakeholders. Understanding ISO 31000's emphasis on risk management is crucial for professionals seeking to establish a solid foundation in managing uncertainties and making informed decisions based on risk assessments.

## 8. What is the impact of non-compliance on an organization's reputation?

- A. Increased customer loyalty
- B. Improved media relations
- C. Loss of trust and customer attrition**
- D. Growth in market share

The impact of non-compliance on an organization's reputation is significant, primarily leading to a loss of trust and customer attrition. When an organization fails to comply with regulatory standards, industry best practices, or internal policies, it can severely damage its credibility with customers, stakeholders, and the general public. This breach can create perceptions of unreliability or negligence, causing customers to question the organization's commitment to ethical practices and quality standards. Consequently, customers may choose to take their business elsewhere, leading to attrition and a diminished customer base. Additionally, the fallout from non-compliance can manifest in negative media coverage, further tarnishing the organization's image and making it more challenging to attract new customers. In contrast, the choices indicating increased customer loyalty, improved media relations, or growth in market share do not correlate with the consequences of non-compliance, as these outcomes would more likely arise from effective compliance and responsible management.

**9. How does risk management integrate with compliance efforts?**

- A. By avoiding any connection between the two
- B. By helping to identify risks that could impact compliance**
- C. By solely focusing on financial risks
- D. By providing legal representation

Risk management integrates with compliance efforts primarily by helping to identify risks that could impact compliance. This relationship is crucial because compliance requirements often stem from regulatory mandates that aim to mitigate risks to information security, privacy, and operational integrity. Through risk management processes, organizations can identify potential vulnerabilities and threats that might prevent them from meeting these compliance obligations. By assessing and evaluating risks, organizations can prioritize their compliance efforts based on potential impacts. For instance, identifying that there is a risk of data breaches can prompt the organization to enhance its compliance strategies related to data privacy laws, such as GDPR or HIPAA. This proactive approach allows organizations to allocate resources effectively to areas where compliance is most critical due to associated risks. The other options do not accurately reflect the relationship between risk management and compliance. Avoiding any connection between the two would undermine the effectiveness of compliance programs, as they rely on an understanding of risks. Focusing solely on financial risks neglects the broader range of compliance-related risks, which can include operational, strategic, and reputational factors. Providing legal representation is not a core function of integrating risk management with compliance, as it does not address the identification and mitigation of risks that could lead to compliance failures.

**10. ISO/IEC 27001 specifies requirements for which of the following?**

- A. Data encryption
- B. Information security management**
- C. Software testing
- D. Environmental management

ISO/IEC 27001 is an international standard that outlines the requirements for an information security management system (ISMS). This standard provides a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability. The main objective of ISO/IEC 27001 is to help organizations manage their information security risks effectively. It establishes a framework for implementing, maintaining, and continually improving the ISMS, which includes policies, processes, and procedures. Organizations that comply with ISO/IEC 27001 can better manage their cybersecurity risks and comply with legal and regulatory requirements related to information security. The other choices do not align with the focus of ISO/IEC 27001. Data encryption is a specific technical measure that can be part of security management but is not the overarching requirement of the standard. Software testing pertains to quality assurance processes but does not relate to a management system for information security. Environmental management, although important for sustainability, is covered under a different set of standards such as ISO 14001 and is not relevant to ISO/IEC 27001.

## 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](mailto: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