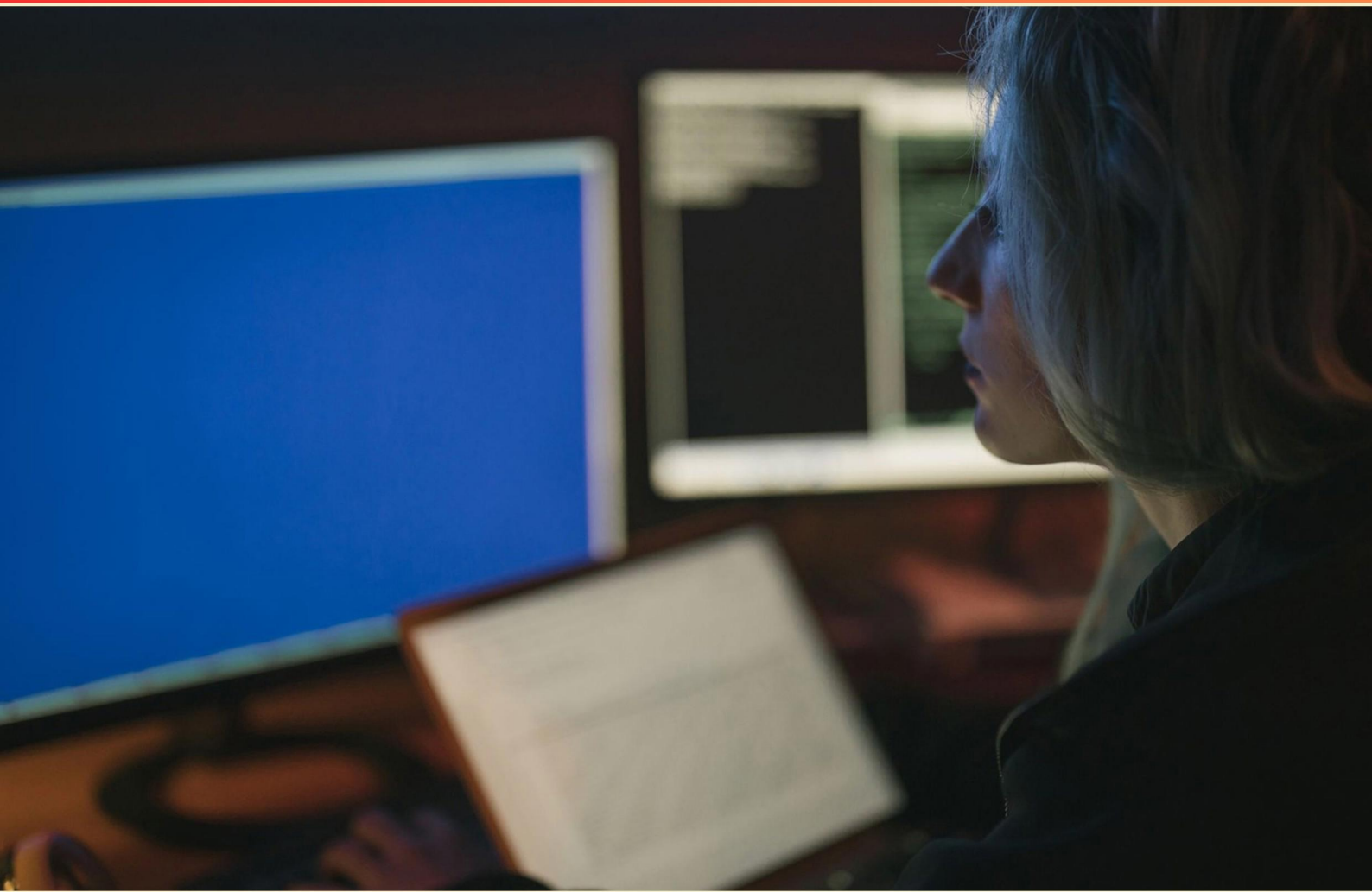


CRISC DOMAIN 1 PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR
THE FULL VERSION STUDY GUIDE

<https://criscdom1.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.

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. Auditing processes are connected to accountability to determine if risk owners are meeting governance and risk management requirements. Which outcome best captures this linkage?**
 - A. Regulatory Enforcement
 - B. Strategic Realignment
 - C. Accountability Through Auditing
 - D. Operational Efficiency
- 2. What is the best approach to develop risk scenarios?**
 - A. Bottom-up approach
 - B. Hybrid approach
 - C. Top-down-bottom-up approach
 - D. Top-down approach
- 3. Who typically reviews and approves the risk register?**
 - A. The CIO
 - B. The risk owner or governance committee (risk management team) depending on the organization.
 - C. The external auditor
 - D. The data steward.
- 4. Which of the following would be considered a vulnerability?**
 - A. A ransomware attack targeting a system.
 - B. A threat actor attempting to breach the network.
 - C. A business process misalignment with objectives.
 - D. Unpatched software that could be exploited.
- 5. What term describes the amount of risk an organization is willing to accept to achieve its goals, in alignment with strategy?**
 - A. Risk Appetite
 - B. Risk Tolerance
 - C. Due Diligence
 - D. Asset Management

- 6. Why is maintaining an up-to-date asset inventory critical in risk management?**
- A. It ensures identified risks reference actual assets and reduces blind spots in risk identification.
 - B. It automatically guarantees regulatory compliance.
 - C. It eliminates the need for risk assessment.
 - D. It speeds up project delivery.
- 7. How do you differentiate between threat and vulnerability in risk identification?**
- A. A threat is a potential cause of harm; a vulnerability is a weakness that could be exploited by a threat.
 - B. A vulnerability is a potential cause of harm; a threat is a weakness.
 - C. A threat is a control to prevent harm.
 - D. A vulnerability is the likelihood of an event.
- 8. How does a risk scenario differ from a risk event?**
- A. A scenario describes a potential sequence leading to an event.
 - B. The event is the actual occurrence after it happens.
 - C. A scenario describes a potential sequence leading to an event, while the event is the potential occurrence itself.
 - D. A scenario is a substitute for a risk treatment plan.
- 9. What is the term for the maximum amount of risk an entity can absorb while pursuing strategy and objectives?**
- A. Risk Appetite
 - B. Risk Tolerance
 - C. Organizational Assets
 - D. Risk Capacity
- 10. What is a common deliverable of risk identification at Domain 1?**
- A. A detailed compliance report.
 - B. A data flow diagram.
 - C. A security control matrix.
 - D. A risk profile or risk register with identified risk events, assets, owners, and initial qualitative assessments.

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Auditing processes are connected to accountability to determine if risk owners are meeting governance and risk management requirements. Which outcome best captures this linkage?

- A. Regulatory Enforcement
- B. Strategic Realignment
- C. Accountability Through Auditing**
- D. Operational Efficiency

Auditing acts as an independent check that verifies whether risk owners are following governance and risk management requirements. By gathering evidence, evaluating controls, and reporting findings, audits establish accountability—clearly indicating who is responsible, whether expectations are met, and what actions are needed to address gaps. While regulatory enforcement, strategic realignment, or operational efficiency can result from audit findings, the strongest fit for the linkage between auditing and governance/risk management is accountability through auditing, because the primary purpose is to hold individuals and processes answerable for adherence and outcomes.

2. What is the best approach to develop risk scenarios?

- A. Bottom-up approach
- B. Hybrid approach
- C. Top-down-bottom-up approach**
- D. Top-down approach

Combining strategic insight with granular, asset-level detail gives the most robust risk scenarios. A top-down view starts from business objectives, risk appetite, and external drivers, identifying threats that could derail critical goals and the possible impact if they occur. A bottom-up view delves into assets, processes, and controls, cataloging vulnerabilities, threat vectors, and lessons from past incidents to ground scenarios in what could realistically happen at the ground level. By blending these perspectives, you get scenarios that are both relevant to executive priorities and plausible in day-to-day operations. This hybrid approach helps close gaps that a single perspective might miss—missed strategic connections from a purely bottom-up method or missed operational realities from a purely top-down method. The result is a comprehensive, implementable set of risk scenarios aligned with the organization's risk tolerance and actual control environment.

3. Who typically reviews and approves the risk register?

- A. The CIO
- B. The risk owner or governance committee (risk management team) depending on the organization.**
- C. The external auditor
- D. The data steward.

The main idea being tested is who holds formal accountability for approving the content and status of the risk register. The best fit is the risk owner or the governance committee that oversees risk management. The risk owner is accountable for a specific risk and is responsible for ensuring the register accurately reflects the risk, the controls in place, the rating, residual risk, and the planned actions. The governance body or risk management team provides the broader oversight, validates that the risks align with the organization's risk appetite, and gives formal approval to changes or updates. In many organizations, either the individual risk owner or the governance committee has the authority to approve the register, depending on local structure. Other roles don't fit as the primary approver. The CIO may sponsor or champion risk initiatives, but not typically authorize every entry or change in the register. The external auditor reviews the risk register for assurance and controls, but their role is to independently assess and report, not to approve the register's contents. The data steward focuses on data assets and quality, not on risk governance and approval processes.

4. Which of the following would be considered a vulnerability?

- A. A ransomware attack targeting a system.
- B. A threat actor attempting to breach the network.
- C. A business process misalignment with objectives.
- D. Unpatched software that could be exploited.**

A vulnerability is a weakness in a system, process, or control that could be exploited by a threat actor to cause harm or gain unauthorized access. Unpatched software fits this definition because when known flaws exist and patches are not applied, attackers can exploit those flaws to compromise the system. Patch management is a core part of reducing the attack surface, so applying updates lowers the likelihood of exploitation and the potential impact. The other scenarios describe actions or outcomes rather than inherent weaknesses: a ransomware attack is a malicious incident targeting systems, a threat actor attempting to breach the network is a threat action, and a business process misalignment with objectives is a governance or process issue that may elevate risk but is not a direct vulnerability in the technical sense.

5. What term describes the amount of risk an organization is willing to accept to achieve its goals, in alignment with strategy?

- A. Risk Appetite**
- B. Risk Tolerance
- C. Due Diligence
- D. Asset Management

The main idea here is the amount of risk an organization is willing to accept in order to pursue its goals within its strategic direction. This is captured by risk appetite, a high-level statement from leadership about how much risk the enterprise is prepared to take. It sets the boundaries for decisions, investments, and initiatives, guiding what opportunities to pursue and which risks to avoid or mitigate. Risk appetite can be described qualitatively (conservative, balanced, aggressive) or quantitatively (specific loss thresholds or exposure limits), but the key point is that it reflects the overall stance toward risk in line with strategy. Risk tolerance, on the other hand, deals with acceptable variation around particular objectives or controls and is more specific and operational. Due diligence is the process of investigating a potential deal or partnership before committing resources, and asset management focuses on maintaining and using the organization's assets, not the level of risk the organization is willing to accept. So risk appetite best fits the description.

6. Why is maintaining an up-to-date asset inventory critical in risk management?

- A. It ensures identified risks reference actual assets and reduces blind spots in risk identification.
- B. It automatically guarantees regulatory compliance.
- C. It eliminates the need for risk assessment.**
- D. It speeds up project delivery.

An up-to-date asset inventory anchors risk identification to real assets, which reduces blind spots in risk detection. When you know exactly what assets exist, where they are, who owns them, and how critical they are, you can link each risk to a specific asset rather than guessing at what might be affected. This makes risk assessments more accurate, because vulnerabilities, threats, and impacts are evaluated in the context of actual holdings, interdependencies, and asset criticality. Without current data, you risk missing assets entirely, mischaracterizing the impact of threats, or misallocating controls and resources. The inventory acts as the reliable foundation for prioritizing risk treatment, mapping controls to assets, and ensuring that risk responses align with what you truly have to protect. It's important to note that this inventory does not automatically guarantee regulatory compliance—compliance requires ongoing governance, controls, and evidence collection across processes. It also does not remove the need for risk assessment; the assessment uses the inventory as essential input, but you still need to analyze threats, vulnerabilities, likelihoods, and impacts. And while a good inventory can streamline certain operational activities, it's not primarily about speeding project delivery.

7. How do you differentiate between threat and vulnerability in risk identification?

- A. A threat is a potential cause of harm; a vulnerability is a weakness that could be exploited by a threat.**
- B. A vulnerability is a potential cause of harm; a threat is a weakness.
- C. A threat is a control to prevent harm.
- D. A vulnerability is the likelihood of an event.

In risk identification, understand that a threat is a potential source of harm, something that could cause damage, while a vulnerability is a weakness or gap in a system, process, or control that could be exploited by that threat. The risk arises when a threat can exploit a vulnerability, turning a possible harm into actual impact. For example, an unpatched software vulnerability creates an opening for a malware threat to cause data loss or disruption. This distinction is why the correct description is that a threat is a potential cause of harm and a vulnerability is a weakness that could be exploited by a threat. The other statements mix up these roles—the threat is not a control, the vulnerability isn't the likelihood, and the vulnerability isn't itself a potential cause of harm.

8. How does a risk scenario differ from a risk event?

- A. A scenario describes a potential sequence leading to an event.
- B. The event is the actual occurrence after it happens.
- C. A scenario describes a potential sequence leading to an event, while the event is the potential occurrence itself.**
- D. A scenario is a substitute for a risk treatment plan.

A risk scenario describes a potential sequence of events that could lead to a risk event, while a risk event is the potential occurrence itself. Think of a scenario as a hypothetical storyline—a chain of causes and intermediate steps that could unfold. The event is what could happen as a result of that storyline, the actual occurrence you would be concerned about monitoring or mitigating. For example, a scenario might outline a phishing attack leading to credential theft and then unauthorized data access. The risk event is the unauthorized data access itself—the outcome that could occur if the scenario plays out. This framing helps you analyze not just that a risk could happen, but how it could happen, and what specific outcome you'd focus on preventing or responding to.

9. What is the term for the maximum amount of risk an entity can absorb while pursuing strategy and objectives?

- A. Risk Appetite
- B. Risk Tolerance
- C. Organizational Assets
- D. Risk Capacity**

The term describes the maximum amount of risk an entity can absorb while pursuing strategy and objectives. It reflects the organization's resilience and available resources—capital, liquidity, people, and processes—to withstand losses or adverse events without failing to meet its goals. This is the ceiling for risk-taking: it answers how much risk the organization can survive. Risk appetite is about the willingness to take on risk at a strategic level, not the hard limit. Risk tolerance describes acceptable variances within that capacity for specific areas or objectives, not the overall maximum. Organizational assets refer to resources the entity uses, not the threshold of risk it can endure.

10. What is a common deliverable of risk identification at Domain 1?

- A. A detailed compliance report.
- B. A data flow diagram.
- C. A security control matrix.
- D. A risk profile or risk register with identified risk events, assets, owners, and initial qualitative assessments.**

In risk identification, the goal is to capture potential threats and vulnerabilities in a structured record that can guide further analysis. The most useful deliverable is a risk profile or risk register that documents identified risk events, the assets affected, the owners responsible for managing each risk, and initial qualitative assessments of likelihood and impact. This creates a centralized, actionable view of the risk landscape that can be prioritized and tracked over time, while assigning accountability to specific individuals or roles and providing an early sense of severity. This format matters because it supports consistent communication among stakeholders and serves as the foundation for subsequent steps, such as prioritization, risk response planning, and ongoing monitoring. It also helps distinguish what could go wrong from how to address it, by starting with who owns the risk and how serious it seems at a glance. Other options miss the mark because a compliance report focuses on regulatory requirements rather than the risk landscape; a data flow diagram maps processes and data movement rather than risks; and a security control matrix is typically developed to address identified risks after assessment, linking controls to risk scenarios rather than serving as the initial risk catalog.

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://criscdom1.examzify.com>

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

SAMPLE