

CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL (CRISC) DOMAIN 2 PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR
THE FULL VERSION STUDY GUIDE**

<https://criscdomain2.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. Who is MOST likely responsible for data classification within an enterprise?**
 - A. The data user
 - B. The data custodian
 - C. The data owner
 - D. The system administrator

- 2. Of the following, which control would a risk practitioner recommend to mitigate the risk that personnel who have the ability to change system configuration settings also modify computer operational logs?**
 - A. Authentication
 - B. Segregation of duties
 - C. Authorization
 - D. Shift rotation

- 3. Which provides the MOST valuable input to incident-response efforts?**
 - A. Qualitative analysis of threats
 - B. The annual loss expectancy
 - C. A vulnerability assessment
 - D. Penetration testing

- 4. Which is MOST important during the quantitative risk analysis process?**
 - A. Net present value
 - B. Decision trees
 - C. Expected monetary value
 - D. Statistical analysis

- 5. What is the BEST reason to perform a risk assessment?**
 - A. To determine the current state of risk
 - B. To analyze the effect on the business
 - C. To budget appropriately for needed controls
 - D. To satisfy regulatory requirements

- 6. Which factor should be included when assessing the impact of losing network connectivity for 18 to 24 hours?**
- A. The hourly billing rate charged by the carrier
 - B. Financial losses incurred by affected business units
 - C. The value of the data transmitted over the network
 - D. An aggregate compensation of all affected business users
- 7. When assessing the performance of a critical application server, the MOST reliable assessment results may be obtained from:**
- A. Documentation of performance objectives
 - B. Continuous monitoring
 - C. Activation of native database auditing
 - D. Documentation of security modules
- 8. Which statement best describes the difference between threat analysis and scenario analysis in estimating likelihood?**
- A. Threat analysis alone does not provide sufficient information to estimate likelihood
 - B. Scenario analysis considers only cost implications
 - C. Threat analysis provides precise likelihood estimates
 - D. Scenario analysis ignores controls and vulnerabilities
- 9. IT risk is measured by its:**
- A. level of damage to IT systems
 - B. impact on business operations
 - C. cost of countermeasures
 - D. annual loss expectancy
- 10. To understand the organization's IT risk for annual strategic direction, management should refer to which of the following?**
- A. The risk profile
 - B. A business case
 - C. The risk action plan
 - D. The risk register

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Who is MOST likely responsible for data classification within an enterprise?

- A. The data user
- B. The data custodian
- C. The data owner**
- D. The system administrator

Determining how data should be classified is driven by who has accountability for the data's value, risk, and regulatory obligations. The data owner is the business role that holds that accountability. They understand the data's impact on the organization, the potential consequences of disclosure or misuse, and any legal or contractual obligations tied to the data. Because of this business context, the owner defines the appropriate classification levels, approves classification decisions, and ensures that policies and controls align with the data's sensitivity and criticality. The data custodian handles the practical aspects of managing data according to those classifications—storing, backing up, labeling, and enforcing access controls as directed by policy. They implement the protections but do not set the classification standards themselves. The system administrator keeps the underlying IT environment running and ensures technical controls (like access enforcement and encryption) function properly, but they do not determine how data should be classified. Data users work with the data in day-to-day operations and follow the classifications and controls, rather than deciding how the data should be classified. So, the person most likely responsible for data classification within an enterprise is the data owner, because they provide the business context, risk judgment, and policy direction that define how data should be classified and protected.

2. Of the following, which control would a risk practitioner recommend to mitigate the risk that personnel who have the ability to change system configuration settings also modify computer operational logs?

- A. Authentication
- B. Segregation of duties**
- C. Authorization
- D. Shift rotation

Segregation of duties is used to prevent a single individual from having both the ability to implement changes and to conceal those changes. When the same person can modify system configuration settings and also alter computer operational logs, they have the opportunity to cover up risks or mistakes. By dividing responsibilities—having configuration changes go through a separate, independent process (often with formal approvals and change control) and keeping logging, log integrity, and log review with a different function or team—the possibility of altering logs without detection is greatly reduced. This creates accountability and makes it harder to bypass controls. Authentication confirms who is requesting access, but it doesn't stop someone from holding conflicting duties. Authorization assigns what a person can do, yet if the same person holds both duties, risk remains. Shift rotation helps detect unusual activity over time and reduces reliance on a single individual, but it doesn't eliminate the fundamental problem of one person controlling both the changes and the logs. Segregation of duties directly mitigates that risk by ensuring no one can both implement changes and alter the evidence of those changes.

3. Which provides the MOST valuable input to incident-response efforts?

A. Qualitative analysis of threats

B. The annual loss expectancy

C. A vulnerability assessment

D. Penetration testing

Understanding attacker behavior and plausible threat scenarios provides the most actionable input for incident-response planning. A qualitative threat analysis describes who might attack, what they're capable of, which assets they target, and the methods and indicators they're likely to leave behind. This context helps incident-response teams design effective detection rules, set appropriate alert thresholds, and prioritize containment and recovery actions based on credible threats. It also supports developing incident-response playbooks and communication plans that reflect real-world adversaries and their potential impact. The other inputs add value in different ways but don't drive incident handling as directly. Annual loss expectancy is a financial projection that doesn't guide how to detect or respond to an incident. A vulnerability assessment identifies weaknesses but not how attackers might exploit them in the wild or what to monitor during an incident. Penetration testing shows exploitable paths within a defined scope and time, but it may miss evolving threat techniques, day-zero methods, or the broader threat landscape that shapes timely detection and response.

4. Which is MOST important during the quantitative risk analysis process?

A. Net present value

B. Decision trees

C. Expected monetary value

D. Statistical analysis

Quantitative risk analysis centers on expressing risk in monetary terms so decisions can be made on the expected financial impact. The most important measure for this is the expected monetary value, because it blends how likely an event is with how much it would cost or gain, producing a single dollar figure you can compare across risks. EMV lets you rank risks, prioritize controls, and estimate overall exposure, especially when running simulations or comparing scenarios. While net present value is about overall project profitability, and decision trees or statistical analysis are valuable tools, EMV provides the direct monetary basis that drives risk prioritization and response. For example, a 5% chance of a \$200,000 loss has an EMV of \$10,000, while a 2% chance of a \$600,000 loss has an EMV of \$12,000, making the latter the higher-priority risk to address.

5. What is the BEST reason to perform a risk assessment?

A. To determine the current state of risk

B. To analyze the effect on the business

C. To budget appropriately for needed controls

D. To satisfy regulatory requirements

A risk assessment is about establishing the current risk exposure for information assets by identifying threats, vulnerabilities, and their likely impact so you understand the present risk state. This baseline is essential because it determines which risks are most significant and where to focus resources for mitigation. Knowing the current risk level allows you to prioritize controls, allocate budgets where they're needed, and set up ongoing monitoring to track how risk changes over time. While budgeting for controls or meeting regulatory expectations can be outcomes of the process, they aren't the primary purpose—the central aim is to know where the organization stands right now in terms of risk.

6. Which factor should be included when assessing the impact of losing network connectivity for 18 to 24 hours?

- A. The hourly billing rate charged by the carrier
- B. Financial losses incurred by affected business units**
- C. The value of the data transmitted over the network
- D. An aggregate compensation of all affected business users

The main idea is to translate a network outage into its monetary impact on the business. When connectivity is down for 18–24 hours, the most meaningful factor to assess is the financial losses incurred by the affected business units. This includes lost revenue, reduced productivity, delayed transactions, and any penalties or costs tied to the downtime. Quantifying these losses per unit helps justify recovery priorities, controls, and investments in resilience (like backups, alternate paths, or faster recovery). The other considerations don't capture the outage's direct financial impact: the carrier's hourly rate is a cost of the service, not the outage's business impact; the inherent value of data being transmitted isn't the loss from not having network access; and compensation to users is about potential liabilities rather than the actual financial impact on the organization during the outage.

7. When assessing the performance of a critical application server, the MOST reliable assessment results may be obtained from:

- A. Documentation of performance objectives
- B. Continuous monitoring**
- C. Activation of native database auditing
- D. Documentation of security modules

Continuous monitoring provides the most reliable insight because it collects real-time, objective data on how the application server performs under actual workloads. It gathers metrics such as response times, throughput, error rates, and resource utilization (CPU, memory, disk I/O, network latency) and stores this historical data to reveal trends and detect anomalies. With baselines and ongoing measurement, you can validate whether performance meets service level objectives, identify bottlenecks, and forecast capacity needs. Documentation of performance objectives is a plan, not evidence of actual performance. Native database auditing focuses on data access events rather than how the application server performs. Documentation of security modules relates to controls rather than performance metrics.

8. Which statement best describes the difference between threat analysis and scenario analysis in estimating likelihood?

- A. Threat analysis alone does not provide sufficient information to estimate likelihood**
- B. Scenario analysis considers only cost implications
- C. Threat analysis provides precise likelihood estimates
- D. Scenario analysis ignores controls and vulnerabilities

The main idea is that threat analysis and scenario analysis serve different roles in estimating likelihood. Threat analysis identifies potential threats and the conditions that could enable them, but it doesn't by itself produce a probability for an event. To estimate how likely an adverse event is, you translate those threats into specific, plausible sequences of events—scenarios—and evaluate how likely each scenario is given the current controls, vulnerabilities, and other factors. That's why threat analysis alone doesn't provide enough information to estimate likelihood: you need the scenario-based view to connect threats to concrete events and probability. For context, scenario analysis looks at how an event could unfold, considering controls and vulnerabilities, and then assesses the probability of those unfolding under real-world conditions. It's not just about costs; it's about the chances of various pathways leading to a risk. Conversely, threat analysis isn't about precise likelihoods; it's about cataloging threats and the conditions that could enable them. And scenario analysis does not ignore controls or vulnerabilities—it uses them to refine how likely a scenario is.

9. IT risk is measured by its:

- A. level of damage to IT systems
- B. impact on business operations**
- C. cost of countermeasures
- D. annual loss expectancy

IT risk is measured by its effect on the business, because risk is about what would happen to the organization's ability to operate and achieve objectives if a threat materializes. The most meaningful measure is the impact on business operations, which captures how service disruption, downtime, revenue loss, compliance issues, and reputational harm would translate into real-world consequences. Technical damage to IT systems is part of the picture, but it doesn't alone reflect how that damage translates into business disruption. The cost of countermeasures speaks to what it costs to mitigate risk, not the risk's severity. Annual loss expectancy is a monetary estimate derived from likelihood and loss but is a quantified outcome, not the primary measure of risk exposure itself.

10. To understand the organization's IT risk for annual strategic direction, management should refer to which of the following?

- A. The risk profile
- B. A business case
- C. The risk action plan

D. The risk register

The central idea is to rely on a centralized, up-to-date record of IT risks and their status to guide annual strategic planning. A risk register collects every identified IT risk, describes its potential impact and likelihood, assigns an owner, lists existing controls and residual risk, and tracks mitigation actions, owner responsibilities, and target dates. This makes it the best source for understanding the current risk posture, what remains unaddressed, and what resources or priorities are needed to align risk with the organization's strategy. It also provides a clear basis for risk reporting to leadership and for monitoring progress over time. A risk profile offers a high-level snapshot and trends, but it usually derives from the underlying register and doesn't substitute for the detailed risk data and action status. A business case justifies a project or investment rather than giving a complete view of IT risk for strategy. The risk action plan outlines steps to address risks but is derived from the register and is not the comprehensive catalog of risks itself.

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://criscdomain2.examzify.com>

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

SAMPLE