CERTIFIED GOVERNANCE RISK AND COMPLIANCE (CGRC) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cgrc.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. **How does a project manager identify risks effectively during the project planning phase?**

   A. By managing stakeholder expectations

   B. By documenting known risks only

   C. By using brainstorming and expert judgment techniques

   D. By ensuring every team member contributes equally

2. **What approach can a project manager take to create a bias against risks affecting the project schedule?**

   A. Pad the team's time estimates

   B. Create an overall project rating scheme

   C. Filter risks based on their effect on schedule

   D. Shift risk-laden activities from the critical path

3. **Which of the following techniques is NOT used as a tool in the qualitative risk analysis process?**

   A. Risk Reassessment

   B. Risk Categorization

   C. Risk Urgency Assessment

   D. Risk Data Quality Assessment

4. **What risk identification approach involves examining the project from four different perspectives?**

   A. SWOT analysis

   B. Root cause analysis

   C. Assumptions analysis

   D. Influence diagramming techniques

5. **What type of accreditation is a part of the NIACAP?**

   A. Employee accreditation

   B. Environmental accreditation

   C. Type accreditation

   D. Level accreditation

SAMPLE

6. What is a key characteristic of certification in the context of information security?

A. Official management decision to authorize operation

B. Assessment of security controls in a system

C. Evaluation of organizational security policy

D. Implementation of the security solutions

7. What is the purpose of configuration audits within the SCM process?

A. To secure confidential information

B. To verify compliance with manufacturing standards

C. To ensure that all configurations are correct

D. To oversee financial transactions

8. Which statement correctly describes the role-based access control (RBAC) model?

A. Permissions are uniquely assigned to each user account

B. A user can access resources according to his role in the organization

C. The same permission is assigned to each user account

D. Users access resources based on their seniority

9. Which NIST document gives guidelines for identifying an information system as a National Security System?

A. NIST SP 800-53.

B. NIST SP 800-59.

C. NIST SP 800-53A.

D. NIST SP 800-37.

10. How is risk exposure calculated during quantitative risk analysis?

A. The probability of a risk event plus the impact of a risk event determines the true risk exposure

B. The risk exposure of a risk event is determined by historical information

C. The probability of a risk event times the impact of a risk event determines the true risk exposure

D. The probability and impact of a risk event are gauged based on research and in-depth analysis

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. How does a project manager identify risks effectively during the project planning phase?

A. By managing stakeholder expectations

B. By documenting known risks only

C. By using brainstorming and expert judgment techniques

D. By ensuring every team member contributes equally

Identifying risks effectively during the project planning phase is critical to the overall success of any project. Utilizing brainstorming and expert judgment techniques plays a significant role in this process. Brainstorming encourages a collaborative environment where team members can freely share their ideas and concerns about potential risks, leading to a more comprehensive identification of issues that might not be immediately obvious. Moreover, expert judgment leverages the knowledge and experience of individuals who have dealt with risks in similar projects before. These experts can provide insights based on historical data, industry standards, and best practices, which can help anticipate risks that might otherwise be overlooked. This combination of collaborative discussion and expert insight ensures that a wide array of potential risks is considered, providing a solid foundation for effective risk management throughout the project lifecycle. While managing stakeholder expectations is important for project success, it doesn't directly contribute to the identification of risks. Documenting known risks only limits the perspective on the variety of risks that could be encountered, and requiring equal contribution from every team member might not yield the same breadth of insights, as not all members will have the same level of experience or expertise. Thus, the use of brainstorming and expert judgment techniques stands out as the most effective method to identify risks during project planning.

2. What approach can a project manager take to create a bias against risks affecting the project schedule?

A. Pad the team's time estimates

B. Create an overall project rating scheme

C. Filter risks based on their effect on schedule

D. Shift risk-laden activities from the critical path

Creating a bias against risks that affect the project schedule involves a proactive approach to identifying and addressing potential challenges. Using an overall project rating scheme is a strategic way to evaluate the magnitude of various risks and prioritize them based on their potential impact on the project's schedule. This method facilitates a comprehensive assessment of the risks, enabling the project manager to decide which risks require immediate attention and which could be monitored over time. Implementing a rating scheme allows the team to quantify risks and their potential influence on the timeline. By systematically categorizing the risks, the project manager gains visibility into how different factors may jeopardize timely project delivery. The rated risks can then be targeted for mitigation strategies or additional resource allocation, helping to minimize potential disruptions to the schedule. In contrast, padding the team's time estimates may not accurately address the risk itself and could lead to complacency. Filtering risks based only on their effect on the schedule could overlook interconnected risks affecting other project aspects. Shifting risk-laden activities from the critical path may provide a temporary solution, but it does not eliminate the underlying risks or their potential consequences on overall project success. Thus, the overall project rating scheme stands out as a comprehensive approach to establishing a bias against schedule-related risks.

SAMPLE

3. Which of the following techniques is NOT used as a tool in the qualitative risk analysis process?

A. Risk Reassessment

B. Risk Categorization

C. Risk Urgency Assessment

D. Risk Data Quality Assessment

In qualitative risk analysis, various techniques are utilized to assess and prioritize risks based on their likelihood and impact. Risk reassessment typically occurs after initial risk analysis and helps to update existing risk evaluations as new information becomes available or conditions change. However, it is not included as a technique used in the initial qualitative risk analysis process. Risk categorization, risk urgency assessment, and risk data quality assessment are fundamental techniques employed during this initial analysis. Risk categorization helps to group risks based on common characteristics, making it easier to manage and communicate them. Risk urgency assessment is used to determine the immediate priority of risks, allowing organizations to focus on the most pressing threats. Meanwhile, risk data quality assessment ensures that the information used for risk analysis is accurate and reliable. These techniques contribute significantly to building a robust framework for identifying and managing risks effectively from the outset.

4. What risk identification approach involves examining the project from four different perspectives?

A. SWOT analysis

B. Root cause analysis

C. Assumptions analysis

D. Influence diagramming techniques

The approach that involves examining a project from four different perspectives is SWOT analysis. This method assesses the Strengths, Weaknesses, Opportunities, and Threats related to a project or organization. By analyzing these four components, teams can identify a comprehensive set of risks and strategic advantages that might affect project outcomes. Strengths and weaknesses focus on internal factors, helping teams to understand what the organization does well and what areas need improvement. Opportunities and threats, on the other hand, look at external factors that could impact the project, such as market trends or competitive pressures. This holistic view enables better risk identification and can inform proactive decision-making in governance, risk management, and compliance efforts. In contrast, root cause analysis focuses specifically on identifying the underlying reasons for specific problems or defects, which does not provide a broad perspective. Assumptions analysis examines assumptions made within project plans but does so in a less structured manner than SWOT. Influence diagramming helps visualize the relationships between variables but does not systematically address the project from multiple dimensions like SWOT does. Therefore, the comprehensive nature of SWOT analysis makes it the correct choice for this question.

SAMPLE

5. What type of accreditation is a part of the NIACAP?

A. Employee accreditation

B. Environmental accreditation

C. Type accreditation

D. Level accreditation

The correct choice is type accreditation, which is integral to the National Information Assurance Certification and Accreditation Process (NIACAP). This process involves a structured approach to certifying and accrediting information systems, emphasizing the importance of evaluating the overall compliance of a system with established security standards. Type accreditation focuses on the system's design and the management controls in place, ensuring that they are suited to meet specific security requirements before the system is operational. In the context of NIACAP, type accreditation verifies that a particular type of system meets the necessary security baseline for the category it belongs to. It differentiates from other forms of accreditation, such as level accreditation, which might pertain to organizations rather than specific systems. While employee and environmental accreditations deal with different aspects, they do not pertain specifically to the structured accreditation framework that NIACAP implements. Understanding the concept of type accreditation is pivotal in governance risk and compliance, as it highlights the distinct focus on system evaluation and assurance within the information security landscape.

6. What is a key characteristic of certification in the context of information security?

A. Official management decision to authorize operation

B. Assessment of security controls in a system

C. Evaluation of organizational security policy

D. Implementation of the security solutions

A key characteristic of certification in the context of information security is the assessment of security controls in a system. Certification involves a comprehensive evaluation of the information system to determine whether the implemented security controls are effective and meet the specified requirements. This assessment typically includes an examination of the technical, administrative, and physical controls that have been deployed to protect the system and its data. Certification is a crucial part of the risk management framework and is often followed by formal authorization to operate (ATO). It provides a level of assurance that the system's controls are appropriate for the protection of sensitive information. This process not only aids in compliance with various regulatory requirements but also fosters a culture of continuous improvement by identifying areas for enhancement in the security posture of the organization.

SAMPLE

7. What is the purpose of configuration audits within the SCM process?

A. To secure confidential information

B. To verify compliance with manufacturing standards

C. To ensure that all configurations are correct

D. To oversee financial transactions

The purpose of configuration audits within the Software Configuration Management (SCM) process is to ensure that all configurations are correct. Configuration audits are conducted to review the existing configurations of software or systems to verify that they match the specified requirements and standards. This process is essential for maintaining the integrity, reliability, and performance of the products being developed, as incorrect configurations can lead to issues such as software failures or security vulnerabilities. Configuration audits involve checking the current state of the system against the documented configuration baselines, assessing whether any unauthorized changes have occurred, and confirming that the system is operating as intended. By ensuring that all configurations are correct, organizations can reduce risks, enhance quality control, and facilitate proper change management processes. The other options relate to different aspects; securing confidential information, verifying compliance with manufacturing standards, and overseeing financial transactions do not align with the specific focus of configuration audits within SCM. These activities are important in their respective contexts but do not directly pertain to the purpose of auditing software configurations.

8. Which statement correctly describes the role-based access control (RBAC) model?

A. Permissions are uniquely assigned to each user account

B. A user can access resources according to his role in the organization

C. The same permission is assigned to each user account

D. Users access resources based on their seniority

The role-based access control (RBAC) model is designed to regulate access to resources based on the roles assigned to individual users within an organization. This approach means that permissions to access certain resources are not tied to individual user accounts but rather to the roles themselves, which are defined according to job responsibilities and functions within the organization. Therefore, a user can access specific resources when their assigned role includes the necessary permissions. The strength of RBAC lies in its ability to simplify user management and enhance security by ensuring users only have access to information necessary for their roles, thereby reducing the risk of unauthorized access. This is particularly beneficial in large organizations where managing individual permissions for each user would be cumbersome and prone to error. The other options present scenarios that do not accurately reflect how RBAC operates. Each user having uniquely assigned permissions complicates access management and is not the essence of RBAC, which focuses on roles rather than individual accounts. Assigning the same permission to all user accounts ignores the principle of differentiated access based on roles. Additionally, providing access based on seniority does not correspond with the functional and role-oriented nature of RBAC, which emphasizes job functions over hierarchical status.

SAMPLE

9. Which NIST document gives guidelines for identifying an information system as a National Security System?

A. NIST SP 800-53.

B. NIST SP 800-59.

C. NIST SP 800-53A.

D. NIST SP 800-37.

The document that provides guidance on identifying an information system as a National Security System is NIST SP 800-59. This publication offers specific criteria for distinguishing between national security systems and other types of information systems, emphasizing the unique security requirements and risk factors associated with national security missions. NIST SP 800-59 outlines the factors and considerations that should be taken into account when determining if a system falls under the category of national security systems, ensuring that organizations can effectively align their security measures with the necessary federal requirements for safeguarding sensitive information that supports national security operations. This is crucial for ensuring that systems critical to national defense are appropriately classified and protected. The other NIST publications listed serve different purposes: NIST SP 800-53 is focused on security and privacy controls, NIST SP 800-53A provides assessment procedures for those controls, and NIST SP 800-37 addresses the Risk Management Framework. While all these documents are important in the broader context of information security, they do not specifically deal with the classification of systems as national security systems.

10. How is risk exposure calculated during quantitative risk analysis?

A. The probability of a risk event plus the impact of a risk event determines the true risk exposure

B. The risk exposure of a risk event is determined by historical information

C. The probability of a risk event times the impact of a risk event determines the true risk exposure

D. The probability and impact of a risk event are gauged based on research and in-depth analysis

The calculation of risk exposure during quantitative risk analysis is grounded in the understanding of both the likelihood of a risk event occurring and the potential impact it would have if it did occur. Specifically, risk exposure is determined by multiplying the probability of a risk event by the impact of that event. This approach allows organizations to quantify risk in a way that is actionable and measurable. By using this formula, organizations can prioritize risks based on their potential financial impact or other significant consequences. If a risk has a high probability of occurring and a high impact, it would represent a greater risk exposure than a risk with a low probability and low impact. The other choices offered do not accurately reflect how risk exposure is calculated in a quantitative risk analysis framework. While historical information and research can provide context for assessing probability and impact, they do not directly determine risk exposure through a systematic calculation. Instead, they serve as supportive data that informs the assessment process, but the actual risk exposure is mathematically defined as a product of probability and impact.

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://cgrc.examzify.com

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

SAMPLE