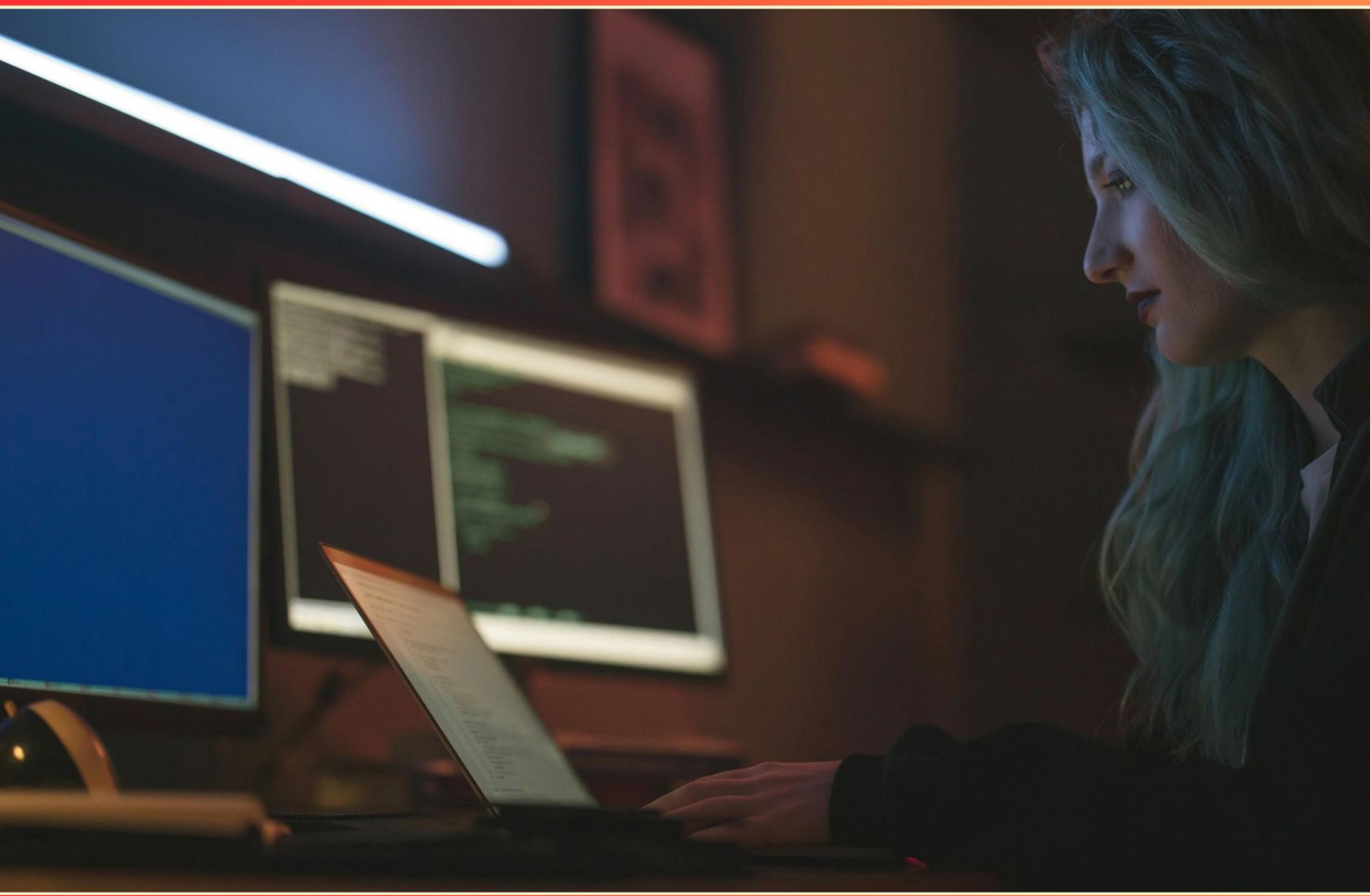
FEDVTE CYBER RISK MANAGEMENT FOR MANAGERS PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://fedvtecyberriskmgmtformngrs.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 does PIA stand for in the context of cybersecurity?

A. Programmatic Information Assessment

B. Privacy Impact Assessment

C. Protected Information Agreement

D. Policy Implementation Approval

2. What is the process of securing a system by reducing its surface of vulnerability called?

A. System hardening

B. Vulnerability assessment

C. Incident response

D. Threat modeling

3. What does TCO stand for in the context of risk management?

A. Total Cost of Ownership

B. Total Cost of Operation

C. Total Control Output

D. Total Compliance Option

4. What security framework focuses on the protection of information systems through layered security strategies?

A. Single Control Strategy

B. Layered Security Model

C. Access Control Model

D. Integrated Security Approach

5. Name one type of risk mitigation strategy.

A. Increasing the number of employees in the IT department.

B. Implementation of security controls.

C. Outsourcing all IT services to third parties.

D. Reducing the size of the organization.

SAMPLE

6. What type of risk is associated with insider threats?

A. Financial risk

B. Operational risk

C. Technical risk

D. Reputational risk

7. Considering TCO helps in understanding what about a security control?

A. Only the financial investment

B. The overall impact on productivity

C. The recurring expenses throughout its use

D. The initial setup requirements

8. What type of risk results from inadequate controls failing to mitigate potential threats?

A. Inherent Risk

B. Control Risk

C. Residual Risk

D. All of the above

9. Identify one key element in the Risk Management Framework.

A. Incident response planning

B. Data encryption techniques

C. Continuous monitoring

D. Network segmentation

10. Which type of security assessment aims to identify vulnerabilities through active testing of systems?

A. Pentest

B. Audit

C. Risk Assessment

D. Compliance Check

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does PIA stand for in the context of cybersecurity?

A. Programmatic Information Assessment

B. Privacy Impact Assessment

C. Protected Information Agreement

D. Policy Implementation Approval

In the context of cybersecurity, PIA stands for Privacy Impact Assessment. This is a process that helps organizations evaluate the effects that a project or system may have on the privacy of individuals and the handling of their personal data. Conducting a PIA is an essential step in identifying potential privacy risks and ensuring compliance with privacy regulations and policies. The Privacy Impact Assessment serves as a tool for organizations to assess how personally identifiable information (PII) is collected, stored, processed, and shared. It also helps to enhance transparency and build trust with stakeholders by demonstrating that the organization takes privacy seriously and is proactively addressing potential risks. By implementing the findings from a PIA, organizations can take necessary steps to mitigate risks to personal information before a project is launched, thus protecting individual privacy rights and reducing the likelihood of data breaches.

2. What is the process of securing a system by reducing its surface of vulnerability called?

A. System hardening

B. Vulnerability assessment

C. Incident response

D. Threat modeling

The process of securing a system by reducing its surface of vulnerability is referred to as system hardening. This practice involves implementing various security measures to protect the system from potential threats. System hardening can include actions such as disabling unnecessary services, configuring security settings, applying patches and updates, and removing unused software. By limiting the number of points where an attacker might exploit vulnerabilities, organizations can significantly decrease the risk of successful cyberattacks. Additional concepts like vulnerability assessment, incident response, and threat modeling play crucial roles in the overall security management framework but focus on different aspects. Vulnerability assessment is aimed at identifying and analyzing vulnerabilities in a system but does not necessarily involve directly hardening it. Incident response pertains to the processes and procedures followed after a security breach occurs, while threat modeling is the practice of identifying and prioritizing potential threats to a system to inform security measures. System hardening specifically addresses the proactive measures taken to minimize vulnerabilities, which is essential in maintaining a robust security posture.

SAMPLE

3. What does TCO stand for in the context of risk management?

A. Total Cost of Ownership

B. Total Cost of Operation

C. Total Control Output

D. Total Compliance Option

In the context of risk management, TCO stands for Total Cost of Ownership. This concept represents the comprehensive assessment of the costs associated with the purchase and ongoing maintenance of a product or system over its entire lifecycle. It goes beyond the initial purchase price to include factors such as installation, operation, maintenance, and potential disposal costs. Understanding TCO is crucial for managers in making informed decisions about investments in technology and security practices, as it provides a clearer picture of the financial implications over time. By evaluating TCO, organizations can identify not only the direct costs but also the indirect costs that might arise from risks such as system downtimes, inefficiencies, and the need for ongoing compliance with regulations. This holistic view helps managers in risk management to prioritize actions that align with both budgetary constraints and risk mitigation strategies.

4. What security framework focuses on the protection of information systems through layered security strategies?

A. Single Control Strategy

B. Layered Security Model

C. Access Control Model

D. Integrated Security Approach

The selected answer emphasizes the layered security model, which is an essential part of modern cybersecurity practices. This framework, often referred to as "defense in depth," advocates for multiple layers of security controls throughout an information system. By implementing various protective measures at different levels, organizations can reinforce their defenses and reduce the likelihood of a successful cyber attack. The layered security model operates on the principle that if one layer fails, others will still be in place to thwart potential threats. This includes a combination of physical security, network security, endpoint security, application security, and user training, among other strategies. Each layer serves a specific purpose and addresses different aspects of security, providing a comprehensive approach to protecting sensitive information. In contrast to other options, the layered security model distinctly stands out by its philosophy of redundancy in security measures. Other options like the single control strategy tend to focus on singular security implementations, while access control models concentrate specifically on restricting access to systems or data. Integrated security approaches may incorporate multiple strategies, but do not emphasize the tiered, layered structure that is characteristic of the layered security model.

SAMPLE

5. Name one type of risk mitigation strategy.

A. Increasing the number of employees in the IT department.

B. Implementation of security controls.

C. Outsourcing all IT services to third parties.

D. Reducing the size of the organization.

Implementation of security controls is a well-established and effective risk mitigation strategy. This approach focuses on reducing vulnerabilities that may expose an organization to potential threats. Security controls can include a range of measures, such as firewalls, intrusion detection systems, access control mechanisms, data encryption, and regular security audits. These controls help create layers of protection that can deter, detect, and respond to cybersecurity incidents, thus significantly lowering the risk profile of an organization. In contrast, the other options may not directly address the risks. For instance, increasing the number of employees in the IT department does not inherently reduce risks unless those additional staff members are effectively trained and involved in implementing and managing security protocols. Outsourcing IT services may transfer some risks but does not fundamentally reduce the inherent cybersecurity risks that need to be managed effectively. Finally, reducing the size of the organization does not necessarily mitigate risks; it may even introduce new vulnerabilities if critical personnel or resources are lost. Therefore, the implementation of security controls stands out as a proactive and focused method for risk mitigation.

6. What type of risk is associated with insider threats?

A. Financial risk

B. Operational risk

C. Technical risk

D. Reputational risk

Insider threats primarily relate to operational risk because they directly impact an organization's day-to-day functioning and processes. Operational risk encompasses the potential for loss resulting from inadequate or failed internal processes, people, or systems. When insiders, such as employees or contractors, intentionally or unintentionally misuse their access to confidential data or systems, it can disrupt operations, lead to financial losses, or compromise sensitive information. Managing insider threats requires a focus on organizational processes, employee training, and monitoring behaviors to minimize operational disruptions. By understanding that insider threats can stem from human error or malicious intent, organizations can develop robust strategies to protect against these risks, thereby ensuring their operational integrity. While financial, technical, and reputational risks may also be consequences of insider threats, the core of the risk is rooted in operational vulnerabilities. For instance, a breach of operational security by an insider could lead to technical failures and subsequently damage the organization's reputation and financial standing, but these are secondary effects resulting from the failure of operational controls.

SAMPLE

7. Considering TCO helps in understanding what about a security control?

A. Only the financial investment

B. The overall impact on productivity

C. The recurring expenses throughout its use

D. The initial setup requirements

Total Cost of Ownership (TCO) provides a comprehensive view of the total costs associated with implementing and maintaining a security control over its lifecycle. This includes not just the initial purchase price or setup expenses but also accounts for ongoing costs such as maintenance, support, training, and any potential operational disruptions caused by the implementation of the control. When evaluating TCO, understanding the recurring expenses is crucial as it allows organizations to assess the long-term financial implications of their security investments. This holistic approach facilitates better budgeting and more informed decision-making regarding resource allocation for security measures. By focusing on all costs associated with a control, rather than just a single aspect, organizations can gain insight into the actual financial burden or value that a security control brings over time, ensuring that they make strategic choices that align with their risk management objectives.

8. What type of risk results from inadequate controls failing to mitigate potential threats?

A. Inherent Risk

B. Control Risk

C. Residual Risk

D. All of the above

The appropriate choice in this scenario is Control Risk. Control Risk specifically refers to the risk that a company's internal controls may fail to prevent or detect errors or irregularities, thus allowing potential threats to manifest. This type of risk emphasizes the effectiveness of the controls in place, highlighting the possibility that controls may not be strong enough to mitigate identified threats adequately. Inherent Risk relates to the level of risk that exists in the absence of any controls. It addresses the natural susceptibility of a given activity, asset, or system to risk, independent of any safeguards or policies. Thus, it does not directly indicate the failure of existing controls. Residual Risk, on the other hand, is the amount of risk that remains after controls have been implemented. It is the leftover risk that the organization still faces, despite having put controls in place to mitigate initial threats. This type of risk assumes that some level of risk is acceptable and will persist even with controls. By identifying Control Risk as the answer, we focus specifically on the potential for inadequate controls to result in vulnerabilities, which is the essence of the question presented.

SAMPLE

9. Identify one key element in the Risk Management Framework.

A. Incident response planning

B. Data encryption techniques

C. Continuous monitoring

D. Network segmentation

Continuous monitoring is a crucial element in the Risk Management Framework as it involves the ongoing assessment of risk and vulnerabilities in an organization's information systems. This process ensures that any changes in security posture or potential threats are identified and addressed in real time. The effectiveness of security controls must be regularly evaluated to ensure they operate as intended and to adapt to the evolving threat landscape. By maintaining continuous monitoring, organizations can proactively detect and respond to incidents, thus enhancing their overall cybersecurity posture and resilience. The other options, while important aspects of cybersecurity, do not encompass the foundational concept of continuous risk evaluation and adjustment that is central to the Risk Management Framework. Incident response planning focuses on procedures and actions to take after a security breach occurs, data encryption techniques safeguard data at rest and in transit, and network segmentation is a strategy to limit exposure and reduce risk. Each of these methods contributes to security, but they are not as pivotal to the overarching, ongoing risk management process as continuous monitoring is.

10. Which type of security assessment aims to identify vulnerabilities through active testing of systems?

A. Pentest

B. Audit

C. Risk Assessment

D. Compliance Check

A penetration test, commonly known as a pentest, is designed to actively test systems for vulnerabilities by simulating an attack. During a pentest, security professionals attempt to exploit weaknesses in a system's defenses, providing a clear picture of how an attacker might gain unauthorized access or cause damage. This assessment not only identifies vulnerabilities but also evaluates the effectiveness of existing security measures, allowing organizations to address those vulnerabilities before they can be exploited maliciously. In contrast, audits typically focus on reviewing policies, procedures, and controls to ensure compliance with regulations and best practices rather than actively testing systems. A risk assessment takes a broader approach, identifying potential risks and their impacts without necessarily performing active testing. Compliance checks ensure that an organization adheres to specific mandates or standards but also do not involve the same level of active testing that a pentest does. Therefore, the primary characteristic that distinguishes a pentest is its focus on actively probing for vulnerabilities in systems, making it the correct choice for this question.

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://fedvtecyberriskmgmtformngrs.examzify.com

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

SAMPLE