(ISC)2 CERTIFIED IN CYBERSECURITY PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR
THE FULL VERSION STUDY GUIDE

https://isc2certifiedincybersecurity.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 term describes events that result in harmful consequences, such as system crashes or unauthorized access?

A. Security Incidents

B. Adverse Events

C. Risks

D. Threats

2. Which control type would focus on the tools and technologies to secure a system?

A. Physical Controls

B. Administrative Controls

C. Technical Controls

D. Compliance Controls

3. What does a security governance framework outline?

A. A list of all employees authorized to access information

B. A framework of policies, procedures, and processes for managing security programs

C. A financial analysis of security expenditures

D. A detailed history of past security incidents

4. What property ensures information is complete, accurate, and useful for its intended purpose?

A. Confidentiality

B. Integrity

C. Availability

D. Reliability

5. What term refers to a message in its natural, readable format that is vulnerable to confidentiality breaches?

A. Plaintext

B. Ciphertext

C. Encrypted text

D. Code

SAMPLE

6. True or False: You are required to report security incidents to law enforcement if you believe a law may have been violated.

A. True

B. False

C. Only if there is evidence

D. Only if it's a significant breach

7. What term describes potential adverse effects on an organization's operations resulting from unauthorized information access?

A. Cyber Threat

B. Information Security Risk

C. Operational Hazard

D. Data Breach Risk

8. During which type of test might teams conduct a complete interruption to their normal business operations?

A. Simulation

B. Full interruption test

C. Walk-through

D. Read-through

9. What does Layer 3 of the OSI model represent?

A. Bit

B. Frame

C. Packet

D. Segment

10. What is the term for the impact of a risk relative to its likelihood?

A. Risk Scope

B. Risk Threshold

C. Risk Evaluation

D. Risk Magnitude

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What term describes events that result in harmful consequences, such as system crashes or unauthorized access?

A. Security Incidents

B. Adverse Events

C. Risks

D. Threats

The term that best describes events leading to harmful consequences, such as system crashes or unauthorized access, is typically referred to as adverse events. These events represent occurrences that negatively impact systems, processes, or services, resulting in detrimental outcomes. In cybersecurity, understanding adverse events is crucial because they highlight the consequences that can arise from vulnerabilities or ineffective security measures. Security incidents generally refer to specific occurrences that actually result in a breach or damage, such as a confirmed hacking attempt, whereas adverse events encompass a broader range of harmful outcomes, including those that may not yet qualify as confirmed incidents but signify a potential setback or compromise. Risks relate to the potential for harm or loss but do not inherently describe an event. Instead, risks are assessed against the likelihood of adverse events occurring and their potential impact. Threats are the potential dangers that could exploit vulnerabilities to cause adverse events; while they are closely related, they do not encompass the actual harmful consequences. Therefore, adverse events more accurately capture the essence of harmful outcomes resulting from such incidents or threats in cybersecurity contexts.

2. Which control type would focus on the tools and technologies to secure a system?

A. Physical Controls

B. Administrative Controls

C. Technical Controls

D. Compliance Controls

Technical controls are designed specifically to implement and enforce security measures using various tools and technologies. These controls include software-based solutions such as firewalls, intrusion detection systems, encryption, and authentication mechanisms. The primary focus of technical controls is to safeguard systems by ensuring that proper security protocols are in place and actively functioning. For instance, technical controls can automatically manage access to a system, monitor for unauthorized attempts to breach security, and protect data through encryption methods. Their effectiveness relies on the deployment of technology to mitigate vulnerabilities, manage risks, and enhance the overall security posture of an organization. While physical controls pertain to tangible barriers and security measures (like locks, security guards, and surveillance cameras), and administrative controls refer to policies, procedures, and practices established to manage organizational security, these do not focus directly on the technologies used for securing systems. Compliance controls involve adherence to laws and standards, which are also not technology-focused. Thus, the emphasis of technical controls distinctly sets them apart as the correct option for this question.

SAMPLE

3. What does a security governance framework outline?

A. A list of all employees authorized to access information

B. A framework of policies, procedures, and processes for managing security programs

C. A financial analysis of security expenditures

D. A detailed history of past security incidents

A security governance framework outlines a structured approach to establishing and maintaining security practices throughout an organization. This includes defining the policies, procedures, and processes necessary for managing security programs effectively. By creating a comprehensive framework, organizations can ensure that their security measures align with their business objectives, comply with regulations, and mitigate risks effectively. This framework serves as a guiding document for the overall security strategy, ensuring that all aspects of security management are considered in decision-making processes. It helps stakeholders understand their roles and responsibilities regarding cybersecurity, facilitates communication across departments, and ensures that there is a consistent and proactive approach to managing security threats. In contrast, the other options focus on specific aspects or components of security and do not encompass the broad, systematic framework that governs security practices: - A list of all employees authorized to access information relates specifically to access control, which is a component of security but does not represent a comprehensive governance framework. - A financial analysis of security expenditures looks at budgeting and resource allocation but does not provide a holistic view of security governance. - A detailed history of past security incidents can be valuable for learning and improving responses, but it does not constitute a framework for managing security in an ongoing, systematic manner. Thus, focusing on policies, procedures, and processes for

4. What property ensures information is complete, accurate, and useful for its intended purpose?

A. Confidentiality

B. Integrity

C. Availability

D. Reliability

The property that ensures information is complete, accurate, and useful for its intended purpose is integrity. In the context of cybersecurity and information management, integrity refers to the assurance that data is trustworthy and untampered with. This means that the information remains in its original state and is not altered, whether accidentally or maliciously. When integrity is maintained, users can trust that the information they are relying on reflects the true state of affairs and can make decisions based on that data confidently. This directly aligns with the concepts of completeness and accuracy since any change to the data could lead to incorrect conclusions or decisions based on faulty information. Thus, integrity is foundational to ensuring that the information serves its intended purpose effectively. While confidentiality relates to ensuring that information is only accessible to those authorized to use it, and availability ensures that information is accessible when needed, it is integrity that specifically focuses on the correctness and trustworthiness of the information itself. Reliability, while often associated with consistent performance over time, is not explicitly focused on the completeness and accuracy of data used for its intended purpose.

SAMPLE

5. What term refers to a message in its natural, readable format that is vulnerable to confidentiality breaches?

A. Plaintext

B. Ciphertext

C. Encrypted text

D. Code

The term that refers to a message in its natural, readable format is "plaintext." Plaintext is the original text before any cryptographic processes have been applied. It can be easily read and understood, which makes it susceptible to confidentiality breaches. When plaintext is transmitted or stored without any protective measures, such as encryption, it poses a security risk because unauthorized users can access its content without any special tools or knowledge. In contrast, ciphertext is the result of encrypting plaintext; it appears scrambled and unreadable to anyone who does not possess the decryption key. Encrypted text is another way of describing ciphertext, emphasizing the process of encryption that has transformed the original data into a secure format. Finally, the term "code" generally refers to a system of symbols, letters, or words used to represent information. While coding can serve a purpose in obfuscating messages, it is not synonymous with the specific concept of plaintext as it relates to vulnerabilities in confidentiality. Therefore, plaintext accurately captures the essence of the question, emphasizing the risks associated with unprotected, readable information.

6. True or False: You are required to report security incidents to law enforcement if you believe a law may have been violated.

A. True

B. False

C. Only if there is evidence

D. Only if it's a significant breach

The assertion that you are required to report security incidents to law enforcement if you believe a law may have been violated is not universally true, which supports the choice of false. Reporting obligations can vary widely depending on the jurisdiction, the type of incident, and the specific laws that may apply. In many cases, organizations may have discretion regarding whether to report certain incidents to law enforcement based on their internal policies, the nature of the violation, or the potential impact of the incident. For example, if sensitive personal information is exposed, there may be legal obligations to notify affected individuals but not necessarily law enforcement unless a crime is clearly evident. Additionally, factors such as the severity of the incident, the potential for ongoing harm, and the organization's specific compliance requirements can also influence whether a report is made. These nuances reflect how different situations may dictate different responses, highlighting the importance of understanding legal obligations in cybersecurity practices. Thus, reporting to law enforcement is not a blanket requirement but rather a decision that may depend on a variety of situational factors. This reinforces the choice to consider the statement false.

SAMPLE

7. What term describes potential adverse effects on an organization's operations resulting from unauthorized information access?

A. Cyber Threat

B. Information Security Risk

C. Operational Hazard

D. Data Breach Risk

The term that most accurately describes the potential adverse effects on an organization's operations due to unauthorized information access is Information Security Risk. This concept encompasses the variety of negative consequences that could arise from threats exploiting vulnerabilities within an organization's systems, particularly regarding the confidentiality, integrity, and availability of sensitive data. Information Security Risk covers a broad range of issues, including data breaches, loss of data integrity, and impacts on operational processes, all of which can significantly affect an organization's ability to function securely and efficiently. It emphasizes not just the act of unauthorized access but also the potential ramifications that such an event could bring about. While the other options touch on related concepts, they do not capture the full scope of potential impacts encompassed by Information Security Risk. For instance, a Cyber Threat refers more to the malicious entities or actions that could exploit vulnerabilities, rather than the resulting effects on the organization itself. An Operational Hazard might imply a risk associated with operational activities, not specifically tied to information security. Data Breach Risk focuses narrowly on the consequences of data breaches alone, without considering the broader risk spectrum related to all unauthorized access scenarios.

8. During which type of test might teams conduct a complete interruption to their normal business operations?

A. Simulation

B. Full interruption test

C. Walk-through

D. Read-through

The full interruption test is conducted when teams deliberately stop all normal business operations to assess the effectiveness of their disaster recovery or business continuity plans. This type of testing is critical because it allows organizations to evaluate their response to a significant disruption and determine how well they can recover essential functions during a real incident. During a full interruption test, participants engage in real-world scenarios that mimic a crisis, allowing them to practice their decision-making, communication, and recovery strategies under pressure. This testing type provides valuable insights into weaknesses in the current plans and helps organizations make necessary adjustments to ensure a more robust recovery process. In contrast, simulation tests typically involve scenario-based exercises without halting business operations, allowing teams to react to a crisis in a controlled environment. Walk-throughs involve discussing procedures and reviewing documentation with no actual disruption, while read-throughs usually consist of reviewing plans or protocols without any involvement from the operational environment. These alternatives do not entail the same level of interruption or practical experience as a full interruption test.

SAMPLE

9. What does Layer 3 of the OSI model represent?

A. Bit

B. Frame

C. Packet

D. Segment

Layer 3 of the OSI (Open Systems Interconnection) model is known as the Network Layer. This layer is primarily responsible for the delivery of packets from the source host to the destination host across multiple networks. It provides routing, forwarding, and addressing functions to ensure that data is transmitted efficiently across different routes. The term "Packet" specifically refers to the data unit that Layer 3 handles. When data is encapsulated for transmission, it progresses through several layers, with each layer adding its own header information. At the Network Layer, the data is encapsulated into packets, which include source and destination IP addresses, allowing the data to traverse across different networks to reach its intended destination. In contrast, the other terms listed pertain to different layers of the OSI model. A "Bit" refers to the physical Layer (Layer 1) that deals with the transmission and reception of raw binary data over a physical medium. A "Frame" is associated with Layer 2, the Data Link Layer, which is concerned with node-to-node data transfer and includes headers that enable devices on the same local area network (LAN) to identify each other. A "Segment" is related to Layer 4, the Transport Layer, which is responsible for

10. What is the term for the impact of a risk relative to its likelihood?

A. Risk Scope

B. Risk Threshold

C. Risk Evaluation

D. Risk Magnitude

In the context of risk management, the term that captures the impact of a risk relative to its likelihood is often referred to as "Risk Magnitude." This concept involves assessing both the potential severity of an impact (the consequences) that could arise if a risk event occurs and the probability of that event occurring. Understanding risk magnitude is crucial because it allows organizations to prioritize risks based on their significance. If a risk is highly likely to occur and could have a severe impact, it demands immediate attention and mitigation strategies. Conversely, a risk that is unlikely to occur, regardless of its potential impact, may be monitored but doesn't require the same level of proactive management. The other options do not effectively define the relationship between impact and likelihood in the same way. For instance, "Risk Scope" refers to the breadth of risk exposure or the range of potential impacts and is not primarily focused on the relationship between likelihood and impact. "Risk Threshold" indicates the level of risk that an organization is willing to accept before taking action, while "Risk Evaluation" is the process of assessing risks and determining their nature and significance rather than specifically relating to the concept of risk impact relative to its likelihood.

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://isc2certifiedincybersecurity.examzify.com

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

SAMPLE