(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

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. **Which of these processes is often synonymous with decryption?**

   A. Encoding

   B. Deciphering

   C. Encrypting

   D. Decrypting

2. **What is the objective of a security incident response communication plan?**

   A. To encrypt data during incidents

   B. To outline communication during a security incident

   C. To analyze security events

   D. To log user access to data

3. **Which classification best fits the activities mandated by the PCI Council for merchants?**

   A. Standard

   B. Guideline

   C. Policy

   D. Protocol

4. **What does cryptography primarily deal with?**

   A. Increasing data storage capacity

   B. Ensuring data access permissions

   C. Securing content and messages

   D. Improving programming languages

5. **Why was Gary locked out of the production environment after three failed login attempts?**

   A. He is being punished

   B. The network is tired

   C. Users remember their credentials if they get time to think

   D. His actions resemble an attack

SAMPLE

6. What is the purpose of security control validation?

A. Identifying new security technologies

B. Testing the effectiveness of security controls

C. Creating a security governance committee

D. Implementing employee training programs

7. What is the main purpose of an Incident Response plan?

A. To enhance web development techniques

B. To outline procedures for responding to security incidents

C. To analyze customer feedback

D. To perform regular financial audits

8. Which characteristic of information ensures it is accessible to authorized users only?

A. Confidentiality

B. Integrity

C. Availability

D. Authenticity

9. In the context of networking, what does 'broadcast' refer to?

A. A form of encrypted transmission

B. A form of data compression

C. A communication method for multiple recipients

D. A method of secure file transfer

10. What does a 'wet pipe system' refer to in fire protection?

A. Active sprinkler system pre-filled with water

B. Inactive water system

C. Fire extinguishers filled with water

D. Water purification systems

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which of these processes is often synonymous with decryption?

A. Encoding

B. Deciphering

C. Encrypting

D. Decrypting

The process that is often synonymous with decryption is deciphering. Decryption refers to the method of converting encoded or encrypted information back into a readable format, while deciphering specifically describes the act of interpreting or making sense of coded language or information. In the context of cryptography, when information is encrypted, it is transformed into a format that is unreadable to anyone who does not possess the appropriate key or method to reverse the transformation. Deciphering represents the broader term that encompasses the action of restoring the original message from the encrypted form. While the term "decrypting" may seem similar, it specifically refers to the technical process of reversing encryption rather than broadly interpreting code. Encoding refers to transforming data into a specific format for transmission or storage and is not directly related to decryption or deciphering. Encrypting is the process of converting plaintext into ciphertext to secure the data and is the opposite of decryption. Hence, deciphering is the most accurate term that aligns with the concept of decryption in this context.

2. What is the objective of a security incident response communication plan?

A. To encrypt data during incidents

B. To outline communication during a security incident

C. To analyze security events

D. To log user access to data

The objective of a security incident response communication plan is to outline communication during a security incident. This plan is essential for ensuring that everyone involved understands their roles, responsibilities, and the protocols for sharing information both internally within the organization and externally with stakeholders, such as law enforcement or the public. Effective communication during a security incident is critical for maintaining situational awareness, coordinating response activities, managing public relations, and ensuring that accurate information is disseminated timely. By having a clear communication plan in place, organizations can minimize confusion and optimize their response efforts, leading to a more efficient resolution of the incident and potentially reducing the impact on the business. The other options focus on aspects that, while important, do not directly relate to the communication strategies required during an incident. Encrypting data during incidents pertains to data protection rather than communication, analyzing security events refers to the post-incident review process, and logging user access to data is a part of data management and security monitoring, not incident communication.

SAMPLE

3. Which classification best fits the activities mandated by the PCI Council for merchants?

A. Standard

B. Guideline

C. Policy

D. Protocol

The activities mandated by the PCI Council for merchants best fit the classification of "Standard." The Payment Card Industry Data Security Standard (PCI DSS) is specifically designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. These standards include a set of requirements that are mandatory for compliance, reflecting the must-do nature of the activities outlined by the PCI Council. Standards are formalized, consistent requirements that organizations must adhere to in order to meet compliance criteria. In this context, the PCI DSS establishes specific technical and operational requirements that merchants need to implement to protect cardholder data, which is crucial for maintaining security in payment card transactions. The other classifications, while relevant to security and compliance discussions, do not carry the same binding nature as a standard. Guidelines offer best practices and recommendations but do not require adherence in the same way. Policies set organizational intent and principles but are broader in scope. Protocols would generally refer to agreed-upon procedures for technical communications and operations, which does not accurately encapsulate the comprehensive mandate provided by PCI standards for merchants. Thus, "Standard" conveys the requirement and the compliance obligation that aligns with PCI Council's intentions.

4. What does cryptography primarily deal with?

A. Increasing data storage capacity

B. Ensuring data access permissions

C. Securing content and messages

D. Improving programming languages

Cryptography primarily deals with securing content and messages, which is essential for protecting information from unauthorized access and ensuring that only intended recipients can read or modify it. The primary goal of cryptography is to maintain the confidentiality, integrity, and authenticity of data. This is achieved through various techniques such as encryption, where data is transformed into a format that is unreadable without a specific key. With cryptography, even if data is intercepted during transit, it remains unintelligible to anyone who does not have the appropriate decryption key. This is crucial in fields like communications, secure transactions, and data storage, where sensitive information must be safeguarded against eavesdropping, tampering, and forgery. While data storage capacity, access permissions, and programming languages are all relevant aspects of information technology and cybersecurity, they do not encompass the primary focus of cryptography, which is fundamentally about protecting the content and ensuring secure communication.

SAMPLE

5. Why was Gary locked out of the production environment after three failed login attempts?

A. He is being punished

B. The network is tired

C. Users remember their credentials if they get time to think

D. His actions resemble an attack

The correct answer is that Gary's actions resemble an attack. In many cybersecurity systems, a common security measure known as "account lockout" is implemented to prevent unauthorized access. When a user exceeds a predetermined number of failed login attempts, the system assumes suspicious activity might be occurring and automatically locks the account to prevent potential malicious actions, such as brute force attacks. In this scenario, failing to log in correctly three times could lead the system to interpret Gary's unsuccessful attempts as indicative of an attempted unauthorized access or attack. This is a proactive approach to enhance security by reducing the risk of compromise to user accounts. The other options present less relevant context. For example, being punished does not align with security best practices, and referring to the network being "tired" personifies technology in a way that is not applicable to user authentication systems. The option about users remembering their credentials if given time does not directly relate to the reasoning behind locking out an account, as the security measure is focused more on preventing unauthorized access rather than assisting users in remembering passwords.

6. What is the purpose of security control validation?

A. Identifying new security technologies

B. Testing the effectiveness of security controls

C. Creating a security governance committee

D. Implementing employee training programs

The purpose of security control validation is centered around testing the effectiveness of security controls. This process involves systematically assessing whether the implemented security measures are operating as intended and effectively mitigating risks. By validating security controls, organizations can ensure that their security strategies align with their risk management objectives and provide the necessary protection against potential threats. This validation process helps to identify any weaknesses or lapses in security that may have gone unnoticed. It ensures a proactive approach to cybersecurity, allowing for adjustments and improvements in security posture before incidents occur. Ultimately, this contributes to a more robust overall security framework, as the organization is better equipped to defend against adversaries. In contrast, the other options focus on distinct elements of a cybersecurity program but do not address the specific purpose of validating security controls. Identifying new security technologies pertains to the ongoing evolution of security solutions rather than assessing existing controls. Creating a security governance committee involves oversight and management but lacks the direct focus on control effectiveness. Implementing employee training programs is essential for fostering a security-aware culture but is not related to the validation process itself. Thus, testing the effectiveness of security controls stands as the correct and most relevant answer.

SAMPLE

7. What is the main purpose of an Incident Response plan?

A. To enhance web development techniques

B. To outline procedures for responding to security incidents

C. To analyze customer feedback

D. To perform regular financial audits

The main purpose of an Incident Response plan is to outline procedures for responding to security incidents. This involves establishing a clear set of actions and protocols that an organization can follow in the event of a cybersecurity incident, such as a data breach, malware attack, or any other security failure. The plan typically includes key components such as detection, containment, eradication, recovery, and lessons learned, enabling teams to respond swiftly and effectively to minimize the impact of an incident. Having a well-defined Incident Response plan is critical for organizations as it not only helps in promptly addressing and managing incidences but also aids in mitigating risks and reducing recovery time and costs associated with incidents. By clearly defining roles, responsibilities, and communication strategies within the organization, the plan ensures that everyone knows what to do when a security issue arises, thereby enhancing overall cybersecurity readiness.

8. Which characteristic of information ensures it is accessible to authorized users only?

A. Confidentiality

B. Integrity

C. Availability

D. Authenticity

The characteristic of information that ensures it is accessible only to authorized users is confidentiality. Confidentiality is a fundamental principle in cybersecurity that focuses on protecting sensitive information from unauthorized access or disclosure. It entails measures that control who can view or access particular data, ensuring that only those individuals or entities with the proper permissions can obtain it. This is achieved through various security measures such as encryption, access controls, and authentication mechanisms, which help to prevent unauthorized users from accessing confidential information. For instance, implementing user authentication processes ensures that only verified individuals can access sensitive systems or data. While the other characteristics—integrity, availability, and authenticity—are also important aspects of information security, they serve different purposes. Integrity ensures that data remains accurate and unaltered by unauthorized individuals. Availability ensures that the information is accessible to authorized users when needed. Authenticity verifies that the information genuinely comes from a recognized source. Each of these principles plays a distinct role in the overall security posture of an organization, but confidentiality specifically addresses the need to restrict access to authorized users alone.

SAMPLE

9. In the context of networking, what does 'broadcast' refer to?

A. A form of encrypted transmission

B. A form of data compression

C. A communication method for multiple recipients

D. A method of secure file transfer

Broadcast refers to a communication method that allows data to be sent to multiple recipients simultaneously within a network. This method is commonly used in various networking scenarios, such as in local area networks (LANs), where a single message sent from one device can be received by all devices connected to that network segment. In a broadcast communication, the sender does not need to send individual messages to each recipient, which enhances efficiency and reduces the overhead associated with message transmission. Broadcast is often utilized in applications such as network discovery protocols and dynamic address resolution protocols, facilitating seamless communication among devices. The other options do not accurately describe broadcast. Encrypted transmission focuses on securing data, data compression pertains to reducing the size of data, and secure file transfer involves methods to safely transfer files over a network. None of these concepts align with the primary characteristic of broadcasting data to multiple recipients at once.

10. What does a 'wet pipe system' refer to in fire protection?

A. Active sprinkler system pre-filled with water

B. Inactive water system

C. Fire extinguishers filled with water

D. Water purification systems

A 'wet pipe system' refers to an active sprinkler system that is pre-filled with water. This means that the pipes in this system contain water at all times, allowing for immediate response to a fire. When a fire is detected, the heat activates the sprinkler heads, which release water directly onto the flames. This system is effective in quickly controlling and suppressing fires, reducing the risk of extensive damage. The other options do not accurately describe what a 'wet pipe system' is. Inactive water systems do not have water available for immediate use in fire protection, while fire extinguishers filled with water are a different method of fire suppression not classified as a wet pipe system. Water purification systems are unrelated to fire protection and focus instead on making water safe for consumption or use. Understanding these distinctions is crucial in recognizing the role and functioning of various fire protection systems.

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