CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cissp.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 technology does a retinal scan utilize?

A. A biometric laser scan of the retina's patterns

B. A camera-based image analysis

C. A fingerprint recognition system

D. A facial recognition protocol

2. What is linear cryptanalysis primarily used for?

A. A known plaintext attack

B. Encrypting data packets

C. Access control management

D. Data compression

3. Which technique does Cross-Site Scripting commonly use?

A. Injecting malicious scripts into webpages

B. Denial of Service attacks

C. Intercepting network traffic

D. Modifying source code directly

4. What does Maximum Transmission Unit (MTU) refer to in networking?

A. The maximum PDU size on a network

B. The minimum required packet size

C. The maximum number of packets sent in a burst

D. The total capacity of a network link

5. What is the primary function of SSL in network communications?

A. To increase data transfer speeds

B. To authenticate and provide confidentiality to network traffic

C. To reduce latency in web applications

D. To manage network protocols

6. What is the purpose of regression testing?

A. To test the security of user authentication

B. To evaluate the performance under load

C. To test software after updates, modifications or patches

D. To assess the usability of software

SAMPLE

7. What does a whitelist typically include?

A. Malicious IP addresses and unauthorized applications

B. Unknown domain names and inactive resources

C. Known good resources such as IP addresses and applications

D. Potentially harmful scripts and programs

8. Which protocol is the full implementation of the 802.11i standard?

A. WPA

B. WPA2

C. WEP

D. TKIP

9. In which OSI layer does the data link layer operate?

A. Layer 1

B. Layer 2

C. Layer 3

D. Layer 4

10. What is the role of Public Key Infrastructure (PKI) in security?

A. To manage user data and credentials

B. To leverage cryptography for digital certificate management

C. To enhance physical security in facilities

D. To store sensitive data securely

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What technology does a retinal scan utilize?

A. A biometric laser scan of the retina's patterns

B. A camera-based image analysis

C. A fingerprint recognition system

D. A facial recognition protocol

A retinal scan fundamentally utilizes a biometric laser scan of the retina's patterns. This technology works by directing low-intensity infrared light into the eye, focusing specifically on the unique patterns of blood vessels in the retina, which are highly distinctive for each individual. This high level of uniqueness and complexity makes retinal scans a reliable method of biometric identification. The importance of this method lies not just in its uniqueness but also in its accuracy; retinal scans are capable of providing a high level of security due to the fact that they require the physical presence of the individual being scanned. This technology is particularly useful in environments where security is critical, such as in financial institutions or secure access areas. In contrast, other technologies mentioned, such as camera-based image analysis or fingerprint recognition systems, operate based on different biometric traits and methodologies. While they have their own merits, they do not involve the biometric scanning of the retina, making them distinct from the retinal scan technology.

2. What is linear cryptanalysis primarily used for?

A. A known plaintext attack

B. Encrypting data packets

C. Access control management

D. Data compression

Linear cryptanalysis is primarily utilized as a known plaintext attack method. This cryptanalytic technique aims to deduce the secret key used in symmetric-key algorithms by exploiting linear approximations of the relationship between the plaintext, ciphertext, and key. In a known plaintext attack scenario, the attacker has access to both the plaintext (the original data) and the corresponding ciphertext (the encrypted data). This knowledge allows them to analyze the transformation that occurs during encryption, thereby revealing patterns or linear relationships that can be exploited to find the key more efficiently than through brute force methods. The other options, such as encrypting data packets, access control management, and data compression, do not relate to the primary purpose of linear cryptanalysis. Encrypting data packets typically involves various encryption algorithms but does not focus on the analytical aspects of deducing keys as linear cryptanalysis does. Access control management pertains to controlling user permissions and access rights rather than the decryption or analysis of cryptographic data. Data compression, on the other hand, involves reducing the size of data for storage or transmission, which is distinctly separate from cryptographic analysis and does not utilize concepts of plaintext and ciphertext relationships in the same way.

SAMPLE

3. Which technique does Cross-Site Scripting commonly use?

A. Injecting malicious scripts into webpages

B. Denial of Service attacks

C. Intercepting network traffic

D. Modifying source code directly

Cross-Site Scripting (XSS) commonly utilizes the technique of injecting malicious scripts into webpages. This vulnerability allows attackers to exploit web applications by inserting harmful JavaScript code, which is then executed in the context of a user's browser. This can lead to unauthorized actions being performed on behalf of the user or sensitive information being stolen, as the malicious script can access cookies, session tokens, or other sensitive data. The primary method of attack is through user input fields or URL parameters, where the malicious script is not properly sanitized or validated by the web application. When other users load the affected page, the injected script executes, compromising user data and session security. Other techniques mentioned, such as Denial of Service attacks, intercepting network traffic, and modifying source code directly, do not accurately describe the typical operation of Cross-Site Scripting. Denial of Service primarily focuses on overwhelming a target system to render it unavailable, while intercepting network traffic deals with capturing data in transit. Modifying source code directly is more aligned with source code vulnerabilities rather than XSS, which exploits client-side execution rather than server-side modification.

4. What does Maximum Transmission Unit (MTU) refer to in networking?

A. The maximum PDU size on a network

B. The minimum required packet size

C. The maximum number of packets sent in a burst

D. The total capacity of a network link

Maximum Transmission Unit (MTU) refers to the maximum size of a protocol data unit (PDU) that can be transmitted over a network medium without requiring fragmentation. This is a critical factor in networking as it determines how much data can be sent in a single packet. The MTU is important because larger PDUs can lead to increased throughput, as fewer packets are needed to send the same amount of data. However, if a packet exceeds the MTU of any segment of the network path, it must be fragmented into smaller packets, which can introduce overhead and slow down transmission. Understanding MTU is essential for network efficiency, as a larger MTU can reduce the overhead caused by headers in network packets, while a smaller MTU may be necessary for compatibility with various types of network equipment or protocols. That's why the concept is focused on the maximum size of the PDU rather than other factors pertaining to network performance such as the number of packets sent or general capacity.

SAMPLE

5. What is the primary function of SSL in network communications?

A. To increase data transfer speeds

B. To authenticate and provide confidentiality to network traffic

C. To reduce latency in web applications

D. To manage network protocols

The primary function of SSL (Secure Sockets Layer) in network communications is to authenticate and provide confidentiality to network traffic. SSL achieves this by establishing an encrypted connection between a client and a server. This encryption ensures that any data transmitted over this connection is protected from eavesdroppers and attackers, making it difficult for unauthorized parties to intercept or decipher the information being exchanged. Additionally, SSL includes mechanisms for authentication, allowing the parties involved in the communication to verify each other's identities. This is crucial in preventing man-in-the-middle attacks, where an unauthorized entity might attempt to impersonate one of the communicating parties. The combination of these features—encryption for confidentiality and authentication for trustworthiness—demonstrates SSL's vital role in securing data transmitted over the internet. The other options focus on aspects that are not the primary functions of SSL. While SSL may contribute to some improvement in performance due to secure connections, its core purpose revolves around security rather than speed or latency. It does not specifically manage network protocols; rather, it operates at a layer that facilitates secure communication over existing protocols.

6. What is the purpose of regression testing?

A. To test the security of user authentication

B. To evaluate the performance under load

C. To test software after updates, modifications or patches

D. To assess the usability of software

The purpose of regression testing is to ensure that software still performs as expected after any updates, modifications, or patches have been made. This type of testing is crucial because changes to the software can inadvertently introduce new bugs or cause existing features to malfunction. By re-running previously conducted tests, regression testing seeks to confirm that the original functionality remains intact and that the new code has not adversely affected the software's overall operation. When updates are applied, especially in complex systems, it's possible for previously functioning components to break due to interactions among different parts of the code. Therefore, regression testing serves as a safeguard to verify that alterations do not have unintended side effects. In contrast, the other options focus on different aspects of software evaluation. Testing the security of user authentication is mainly concerned with access controls and protections against unauthorized access. Evaluating performance under load looks at how the software performs under stress or heavy usage, assessing responsiveness and stability. Assessing usability focuses on how intuitive and user-friendly the software is, which is separate from ensuring that existing functionality is preserved after changes have been made. Each of these areas is essential in software development and maintenance, but they do not address the core aim of regression testing.

SAMPLE

7. What does a whitelist typically include?

A. Malicious IP addresses and unauthorized applications

B. Unknown domain names and inactive resources

C. Known good resources such as IP addresses and applications

D. Potentially harmful scripts and programs

A whitelist is a security mechanism that allows only specified entities to be accessed or executed within a system. This typically includes known good resources such as IP addresses or applications that have been evaluated and deemed safe for use. By maintaining a whitelist, organizations can enhance their security postures by allowing only verified and trusted resources, while all other, unapproved resources are blocked. This approach helps prevent unauthorized access and reduces the risk posed by potential threats. In practice, if an application or IP address is not on the whitelist, it is automatically denied permission to operate or connect, effectively minimizing the attack surface of the network or system. In contrast to other options, malicious IP addresses and unauthorized applications, unknown domain names and inactive resources, as well as potentially harmful scripts and programs, are not permissible entries in a whitelist, as their inclusion would conflict with the fundamental purpose of a whitelist, which is to restrict access to only those entities that have been validated as safe.

8. Which protocol is the full implementation of the 802.11i standard?

A. WPA

B. WPA2

C. WEP

D. TKIP

The full implementation of the 802.11i standard is WPA2. The 802.11i standard was developed to enhance the security of wireless networks and includes provisions for stronger authentication and encryption methods. WPA2 specifically utilizes the Advanced Encryption Standard (AES) for encryption, which is considered much more secure than the methods used in earlier standards. While WPA, the predecessor to WPA2, initially implemented some aspects of the 802.11i standard, it was not fully compliant. WPA used TKIP (Temporal Key Integrity Protocol) as a temporary solution to address vulnerabilities in WEP, which was inadequate for modern security needs. TKIP is not a protocol that fully aligns with 802.11i since it ultimately relies on WEP's underlying weaknesses. WEP itself is an outdated encryption standard that was part of the earlier wireless standards but was intended to provide minimal security. It has since been deemed insecure and is not compliant with the enhancements offered in 802.11i. Thus, WPA2 stands out as the correct answer, as it fully embraces the enhanced security protocols outlined in the 802.11i standard, providing robust authentication and encryption for modern wireless networks.

SAMPLE

9. In which OSI layer does the data link layer operate?

A. Layer 1

B. Layer 2

C. Layer 3

D. Layer 4

The data link layer operates at Layer 2 of the OSI model. This layer is critical as it is responsible for node-to-node data transfer and error detection and correction. It serves as an intermediary layer between the physical layer, which is Layer 1, and the network layer, which is Layer 3. The data link layer takes packets from the network layer and encapsulates them into frames that can be transmitted over the physical layer. Functions of the data link layer include managing how data packets are placed on the physical medium, controlling access to the physical layer, and ensuring reliable communication between devices on the same network segment. By handling tasks such as framing, addressing (using MAC addresses), and error recovery, the data link layer plays a vital role in the overall networking process, working closely with the layers above and below it.

10. What is the role of Public Key Infrastructure (PKI) in security?

A. To manage user data and credentials

B. To leverage cryptography for digital certificate management

C. To enhance physical security in facilities

D. To store sensitive data securely

The role of Public Key Infrastructure (PKI) in security is fundamentally centered around the use of cryptography for managing digital certificates, which is why the choice highlighting this aspect is the correct one. PKI enables secure communications by generating, distributing, and revoking digital certificates that confirm the identities of entities, such as users or devices, within a network. PKI facilitates different cryptographic functions, including encryption and digital signatures, which are crucial for ensuring data integrity, confidentiality, and authenticity in communications. In a PKI system, a trusted authority, known as a Certificate Authority (CA), issues certificates that bind an individual's identity to their public key. This trust model allows users to verify the identity of other users or services before establishing secure connections. The other options do not fully encapsulate the primary function of PKI. While managing user data and credentials is important for an organization's security posture, it does not specifically relate to the central cryptographic role PKI plays. Enhancing physical security in facilities and storing sensitive data securely are also critical components of a comprehensive security strategy, but they fall outside the scope of what PKI is designed to do, which is specifically related to the management and validation of digital certificates and key pairs used in crypt

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://cissp.examzify.com

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

SAMPLE