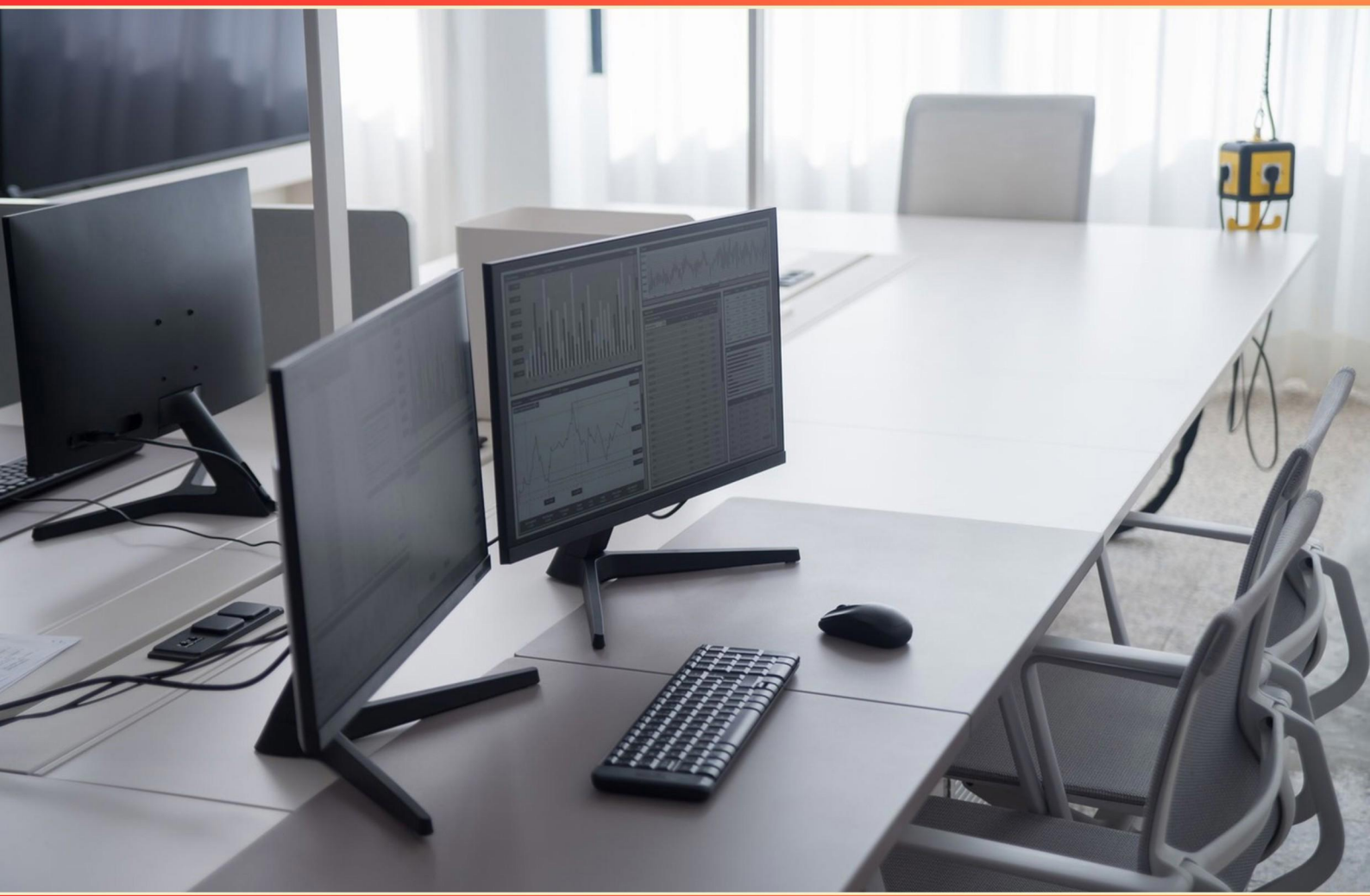
INFORMATION TECHNOLOGY SPECIALIST (ITS) CYBERSECURITY PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://its-cybersecurity.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 the concept of "defense in depth" emphasize in cybersecurity?

A. A layered security approach

B. A single point of security control

C. Minimal use of security measures

D. A focus solely on endpoint protection

2. Which of the following is a primary purpose of a firewall?

A. To log user activity

B. To monitor network traffic

C. To filter incoming and outgoing traffic

D. To encrypt sensitive data

3. Which part of the CIA Triad is compromised by shoulder surfing?

A. Integrity

B. Confidentiality

C. Availability

D. None of the above

4. Describe a "man-in-the-middle" attack.

A. An attack that disrupts service by overwhelming a network with traffic

B. An attack where an unauthorized party intercepts and possibly alters communication between two parties

C. An exploit that takes advantage of software vulnerabilities

D. An attack focused on stealing user credentials through phishing

5. What does the acronym VPN stand for in cybersecurity?

A. Virtual Private Network

B. Visual Public Network

C. Variable Protocol Network

D. Vulnerable Protocol Network

SAMPLE

6. In syslog messages, which field identifies the device experiencing the logged event?

A. Event Type

B. Hostname

C. Severity Level

D. Timestamp

7. Which of the following are two common types of malware?

A. Adware and spyware

B. Virus and ransomware

C. Trojan and firewall

D. Worm and phishing

8. What software enables multiple operating systems to run on the same physical machine?

A. Virtual machines

B. Hypervisor

C. Container

D. Firewall

9. What is the main focus of penetration testing?

A. To ensure software licensing compliance

B. To identify system vulnerabilities that could be exploited by attackers

C. To develop user training sessions

D. To audit company policies

10. What is meant by "security governance"?

A. The framework for establishing security policies, procedures, and controls to manage risks effectively

B. The analysis of network traffic for potential intrusions

C. The process of training staff on security awareness

D. The technology used to monitor physical access to facilities

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does the concept of "defense in depth" emphasize in cybersecurity?

A. A layered security approach

B. A single point of security control

C. Minimal use of security measures

D. A focus solely on endpoint protection

The concept of "defense in depth" emphasizes a layered security approach. This strategy involves implementing multiple layers of security controls throughout the IT environment, rather than relying on a single line of defense. By having various safeguards in place, such as firewalls, intrusion detection systems, antivirus software, and physical security measures, organizations can create a more resilient defense against potential security threats. This multi-faceted approach ensures that if one layer is breached, additional layers remain in place to provide protection. It's designed to address various types of threats and vulnerabilities, allowing for a more comprehensive risk management strategy. Each layer serves as a barrier against attacks, and the combined effect of all layers working together enhances the overall security posture. The other options do not align with the principle of defense in depth. A single point of security control can lead to vulnerabilities if that control is compromised. Minimal use of security measures is contrary to the concept of layering and would increase the risk of a successful attack. Focusing solely on endpoint protection neglects other critical areas of security, such as network defenses and data protection, which are essential components of a robust security strategy.

2. Which of the following is a primary purpose of a firewall?

A. To log user activity

B. To monitor network traffic

C. To filter incoming and outgoing traffic

D. To encrypt sensitive data

The primary purpose of a firewall is to filter incoming and outgoing traffic. Firewalls serve as a barrier between a trusted internal network and untrusted external networks, such as the internet. By analyzing and controlling the data packets that are allowed to enter or exit the network, firewalls help ensure that harmful traffic, such as unauthorized access attempts or malware, is blocked. This filtering process is essential for protecting sensitive information and maintaining the security of a network infrastructure. While other options present important functions in the realm of cybersecurity, they do not capture the primary role of a firewall. For example, logging user activity is typically associated with security information and event management (SIEM) systems rather than firewalls specifically. Monitoring network traffic can be a function of a firewall, but it is not its main purpose; there are dedicated tools for that task. Encrypting sensitive data pertains more to data protection techniques rather than the function of a firewall, which focuses on managing traffic flow rather than directly securing the content of that traffic.

SAMPLE

3. Which part of the CIA Triad is compromised by shoulder surfing?

A. Integrity

B. Confidentiality

C. Availability

D. None of the above

Shoulder surfing primarily compromises confidentiality, which is one of the three essential components of the CIA Triad (Confidentiality, Integrity, Availability) used in the field of cybersecurity. When someone engages in shoulder surfing, they observe a person's actions—such as entering passwords or viewing sensitive information on a screen—without the individual's knowledge. This unauthorized observation allows the shoulder surfer to gain access to confidential information that should be kept private. Confidentiality is all about protecting sensitive information from unauthorized access. When information is exposed through means such as shoulder surfing, it undermines this principle, leading to potential data breaches and unauthorized disclosure of sensitive data. The other components of the CIA Triad—integrity and availability—are not directly impacted by shoulder surfing in the same way. Integrity refers to the accuracy and trustworthiness of data, and availability relates to ensuring that information is accessible to authorized users when needed. In this scenario, shoulder surfing does not inherently alter the data or impact its accessibility, but it clearly poses a risk to confidentiality.

4. Describe a "man-in-the-middle" attack.

A. An attack that disrupts service by overwhelming a network with traffic

B. An attack where an unauthorized party intercepts and possibly alters communication between two parties

C. An exploit that takes advantage of software vulnerabilities

D. An attack focused on stealing user credentials through phishing

A "man-in-the-middle" attack refers to a scenario where an unauthorized party clandestinely intercepts and may alter the communications between two legitimate parties without their knowledge. In this attack, the intruder situates themselves between the sender and receiver, capturing and potentially modifying the data exchanged. This can occur in various forms, including eavesdropping on sensitive information, such as login credentials, or even injecting misleading information into the communication stream, which can have significant consequences for the parties involved. This type of attack can be particularly dangerous because the parties engaged in the communication may not be aware that their exchange is being monitored or manipulated. Techniques often used in such attacks can involve exploiting unsecured networks, such as public Wi-Fi, or employing malicious software that can intercept data transmissions. Understanding the mechanics of a man-in-the-middle attack is crucial for implementing adequate cybersecurity measures, such as encryption, to help safeguard communication channels and ensure data integrity.

SAMPLE

5. What does the acronym VPN stand for in cybersecurity?

A. Virtual Private Network

B. Visual Public Network

C. Variable Protocol Network

D. Vulnerable Protocol Network

The acronym VPN stands for Virtual Private Network. This term refers to a technology that creates a secure and encrypted connection over a less secure network, such as the Internet. VPNs are essential tools in cybersecurity, as they allow individuals and organizations to protect their data from unauthorized access while providing remote access to private networks. The "virtual" aspect indicates that the network can be created over a public infrastructure while maintaining privacy. The term "private" highlights the goal of ensuring that the data transmitted over this network is shielded from eavesdropping and interference. VPNs establish a private tunnel through which data travels, thus providing security against potential threats that could exploit public network vulnerabilities. While the other options use some of the correct terminology and convey network-related concepts, they do not accurately describe the function or nature of a VPN. For instance, "Visual Public Network" does not imply any security aspects, "Variable Protocol Network" suggests a focus on changing protocols rather than security, and "Vulnerable Protocol Network" introduces an erroneous notion of inherent risk within its name, which contradicts the protective purpose of a VPN.

6. In syslog messages, which field identifies the device experiencing the logged event?

A. Event Type

B. Hostname

C. Severity Level

D. Timestamp

The chosen answer accurately identifies the field in syslog messages that indicates the specific device experiencing the logged event. In syslog, the hostname field is crucial as it contains the name of the device or system that generated the log message. This allows administrators and security professionals to pinpoint the source of an event, which is essential for troubleshooting, monitoring, and responding to incidents. Other fields in a syslog message serve different purposes. The event type describes the nature of the event, but it does not specify which device generated it. Severity level indicates the urgency or importance of the event but also does not provide information about the originating device. Lastly, the timestamp records when the event occurred, offering a temporal reference, yet it similarly lacks identification of the device involved. Understanding the function of each field is important for effectively utilizing syslog messages for cybersecurity and IT management.

SAMPLE

7. Which of the following are two common types of malware?

A. Adware and spyware

B. Virus and ransomware

C. Trojan and firewall

D. Worm and phishing

Virus and ransomware are indeed two common types of malware. A virus is a type of malicious software that attaches itself to legitimate programs or files and can spread to other systems when those programs or files are shared. Once activated, viruses can corrupt files, steal data, or cause system failures. Ransomware, on the other hand, is a type of malware that encrypts the victim's data and demands a ransom payment to restore access. Both types impact users significantly, either by disrupting functionality or by exploiting data for financial gain, making them prevalent threats in cybersecurity. Adware and spyware are also forms of malware but serve different purposes: adware displays unwanted advertisements, while spyware gathers information without consent. A Trojan is a type of malware disguised as legitimate software, whereas a firewall is a security device that filters traffic; it is not malware. Lastly, worms are self-replicating malware that can spread across networks, and phishing is a social engineering technique used to deceive users into handing over sensitive information, but it is not classified as malware itself. Hence, while the other answers include some elements of malware, they don't align as clearly with the quintessentially dangerous types highlighted in the context of the question.

8. What software enables multiple operating systems to run on the same physical machine?

A. Virtual machines

B. Hypervisor

C. Container

D. Firewall

The correct answer is hypervisor. A hypervisor is a crucial piece of virtualization technology that allows multiple virtual machines (VMs) to run concurrently on a single physical machine. It acts as an intermediary between the physical hardware and the operating systems, managing the resources and ensuring that each VM operates independently and effectively. Hypervisors can be categorized into two types: Type 1 hypervisors, which run directly on the hardware, and Type 2 hypervisors, which run on a host operating system. This functionality enables organizations to optimize hardware utilization, isolate environments for testing or development, and run multiple OS environments without the need for separate physical computers. While virtual machines are the instances created by the hypervisor, they are not the software that enables the full capability of running multiple operating systems. Containers, on the other hand, are technologies that package software and its dependencies for consistent execution across environments but do not virtualize hardware. A firewall, in contrast, is a security device that monitors and controls incoming and outgoing network traffic, unrelated to running multiple operating systems.

SAMPLE

9. What is the main focus of penetration testing?

A. To ensure software licensing compliance

B. To identify system vulnerabilities that could be exploited by attackers

C. To develop user training sessions

D. To audit company policies

The main focus of penetration testing is to identify system vulnerabilities that could be exploited by attackers. This process involves simulating attacks on a system, network, or web application to detect weaknesses that could be leveraged by malicious actors. By mimicking the tactics, techniques, and procedures of actual attackers, penetration testers aim to uncover security flaws before they can be exploited in a real-world scenario. This proactive approach helps organizations understand their security posture and prioritize remediation efforts on the most critical vulnerabilities, thereby strengthening the overall security of their systems and protecting sensitive data from unauthorized access. Penetration testing not only reveals vulnerabilities but also provides insights into how to mitigate risks and improve security measures. The other options focus on different aspects of cybersecurity management that, while important, do not align specifically with the primary goal of penetration testing, which is centered around identifying exploitable vulnerabilities.

10. What is meant by "security governance"?

A. The framework for establishing security policies, procedures, and controls to manage risks effectively

B. The analysis of network traffic for potential intrusions

C. The process of training staff on security awareness

D. The technology used to monitor physical access to facilities

Security governance refers to the overarching framework and strategic approach an organization adopts concerning its cybersecurity policies, procedures, and controls. This framework ensures that security practices align with the organization's goals and regulatory requirements while effectively managing risks associated with information assets. This concept emphasizes the importance of a structured methodology to establish and maintain security protocols throughout the organization, ensuring that individuals and departments adhere to these standards. By focusing on risk management, security governance helps identify potential threats and vulnerabilities, allowing organizations to allocate resources efficiently to mitigate these risks. In contrast, the other options delve into specific aspects of cybersecurity rather than the broader governance framework. Analyzing network traffic for potential intrusions pertains to operational security measures rather than governance. Training staff on security awareness is an important part of building a security culture but does not encapsulate the managerial oversight that governance involves. Finally, monitoring physical access to facilities falls under physical security controls rather than the strategic, policy-oriented focus of governance.

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://its-cybersecurity.examzify.com

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

SAMPLE