Security Fundamentals Professional Certification (SFPC) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit:
https://securityfundamentalsprofessionalcertification.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. **Which type of briefing reinforces initial security information and communicates updates in security regulations?**
   - **A. Annual Refresher Briefings**
   - **B. Indoctrination Briefings**
   - **C. Attestation Briefings**
   - **D. Courier Briefings**

2. **Which process ensures that critical operations can continue after a disruption?**
   - **A. Disaster Recovery Planning**
   - **B. Business Continuity Planning**
   - **C. Risk Assessment**
   - **D. Incident Management**

3. **What is the primary function of antivirus software?**
   - **A. To detect, prevent, and remove malware from devices**
   - **B. To enhance system performance**
   - **C. To manage user permissions**
   - **D. To secure physical access to hardware**

4. **Which of the following is a benefit of implementing a firewall?**
   - **A. It provides antivirus protection**
   - **B. It helps prevent unauthorized access to a network**
   - **C. It acts as a backup storage device**
   - **D. It enhances internet speed**

5. **According to Executive Order 13556, which of the following is a type of controlled unclassified information?**
   - **A. Communications Security (COMSEC) Information**
   - **B. Declassified Information**
   - **C. Law Enforcement Sensitive Information**
   - **D. NATO Information**

SAMPLE

6. What is phishing considered to be in the realm of cybersecurity?

A. A legitimate email request for information

B. A type of social engineering attack

C. A security protocol for email communication

D. A method to track user online behavior

7. What is Active Directory?

A. A web-based application for managing files

B. A directory service for Windows domain networks

C. A type of virtual private network

D. A security protocol for user authentication

8. Which type of digital footprint is created automatically without user intent?

A. Active digital footprint

B. Passive digital footprint

C. Private digital footprint

D. Public digital footprint

9. What is the ultimate goal of a security policy in an organization?

A. To dictate employee behavior

B. To outline compliance measures

C. To safeguard organizational assets

D. To limit network access

10. What type of system is primarily concerned with detecting and responding to breaches?

A. An Intrusion Prevention System (IPS)

B. An Intrusion Detection System (IDS)

C. A Data Loss Prevention System (DLP)

D. A Security Information and Event Management system (SIEM)

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which type of briefing reinforces initial security information and communicates updates in security regulations?

A. Annual Refresher Briefings

B. Indoctrination Briefings

C. Attestation Briefings

D. Courier Briefings

Annual Refresher Briefings are designed specifically to reinforce initial security information that personnel have received and to update them on any changes or enhancements in security regulations. These briefings serve as a reminder of the foundational knowledge individuals need to maintain a secure environment while also addressing new developments in security practices and compliance standards. This regular engagement is critical in ensuring that employees remain aware of their responsibilities, the importance of adhering to security protocols, and the latest regulatory requirements, which can evolve over time due to changing risks and threats. By incorporating updates and reinforcing previous training, these briefings help maintain a culture of security awareness within an organization. Indoctrination Briefings focus on introducing personnel to the security policies and procedures at their initial entry point rather than providing updates, while Attestation Briefings typically involve an acknowledgment of understanding security policies rather than education or reinforcement. Courier Briefings are specific to delivering sensitive information securely and do not generally cover updates to security policies.

2. Which process ensures that critical operations can continue after a disruption?

A. Disaster Recovery Planning

B. Business Continuity Planning

C. Risk Assessment

D. Incident Management

Business Continuity Planning is a comprehensive process that focuses on ensuring that critical operations of an organization can continue during and after a disruption. This planning involves creating strategies and establishing procedures to maintain essential functions, minimize downtime, and effectively manage resources in the face of unforeseen events such as natural disasters, cyberattacks, or other operational disruptions. The significance of Business Continuity Planning lies in its forward-looking nature, which emphasizes the resilience of operations and the ability to recover quickly. It encompasses various elements such as risk assessment, response strategies, recovery plans, and ongoing training and testing, thus ensuring that organizations are prepared for a range of potential challenges. The goal is to sustain vital services and operations, safeguarding both the organization's interests and its stakeholders. In contrast, Disaster Recovery Planning primarily focuses on the recovery of IT and data systems after a disaster. While it is an essential component of maintaining business continuity, it does not encompass all aspects of the organization's operations. Risk Assessment identifies and evaluates potential risks but does not inherently provide a strategy for ongoing operations during a disruption. Incident Management deals with responding to and managing incidents as they occur but does not necessarily ensure the continuity of critical operations.

SAMPLE

3. What is the primary function of antivirus software?

A. To detect, prevent, and remove malware from devices

B. To enhance system performance

C. To manage user permissions

D. To secure physical access to hardware

The primary function of antivirus software is to detect, prevent, and remove malware from devices. Antivirus software plays a crucial role in cybersecurity, acting as a protective barrier against various forms of malicious software, including viruses, trojans, worms, ransomware, and spyware. It employs various techniques such as signature-based detection, heuristic analysis, and behavior monitoring to identify malicious code before it can cause harm to the system or spread to other devices. This software typically runs in the background, continuously scanning files and programs for known malware signatures or behaviors that indicate suspicious activity. If malware is detected, antivirus software can either quarantine it to prevent it from executing or remove it entirely from the system. By performing these functions, antivirus software helps maintain the integrity, confidentiality, and availability of data and resources on a device. While enhancing system performance, managing user permissions, and securing physical access to hardware are important aspects of cybersecurity and IT management, they do not constitute the primary purpose of antivirus software. These functions pertain to different areas of security and system administration, but they are not the core objective of antivirus solutions. The main focus remains on identifying and mitigating threats posed by malware, thereby providing a safer computing experience for users.

4. Which of the following is a benefit of implementing a firewall?

A. It provides antivirus protection

B. It helps prevent unauthorized access to a network

C. It acts as a backup storage device

D. It enhances internet speed

Implementing a firewall is primarily beneficial for preventing unauthorized access to a network, which is why this option is correct. Firewalls act as a barrier between a trusted internal network and untrusted external networks, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. This helps protect sensitive data and resources from malicious intrusions, effectively reducing the risk of unauthorized access. The other options do not accurately reflect the primary role of a firewall. While antivirus protection is focused on detecting and mitigating malware threats, a firewall's function is to block or allow traffic based on security settings rather than scanning for viruses. Firewalls do not provide backup storage capabilities as they are not designed to store data; their purpose is to regulate network traffic. Additionally, while it may appear that a firewall could enhance internet speed by filtering out potentially harmful traffic, its primary role is not to increase speed but to ensure security. Therefore, the correct choice emphasizes the essential security function of firewalls in network protection.

SAMPLE

5. According to Executive Order 13556, which of the following is a type of controlled unclassified information?

A. Communications Security (COMSEC) Information

B. Declassified Information

C. Law Enforcement Sensitive Information

D. NATO Information

Controlled Unclassified Information (CUI) is a category of unclassified information that requires protection and is not public but does not rise to the level of classified information. Executive Order 13556 established a uniform protocol for managing this type of information within the federal government. Law Enforcement Sensitive Information is indeed a recognized type of CUI because it pertains to law enforcement processes and operations where unauthorized disclosure could compromise law enforcement activities or assist criminals. This classification helps ensure that sensitive information related to investigations or operations is adequately protected while still being unclassified. In contrast, Communications Security (COMSEC) Information is generally classified due to its impact on national security, while declassified information by definition is no longer considered sensitive and does not require any special protection. NATO Information, although sensitive within its context, is also typically treated according to specific agreements and classifications that go beyond the CUI designation under U.S. federal policy. Thus, Law Enforcement Sensitive Information stands as a proper type of CUI under Executive Order 13556.

6. What is phishing considered to be in the realm of cybersecurity?

A. A legitimate email request for information

B. A type of social engineering attack

C. A security protocol for email communication

D. A method to track user online behavior

Phishing is classified as a type of social engineering attack because it exploits human psychology to manipulate individuals into divulging sensitive information, such as usernames, passwords, and credit card details. This manipulation often occurs through deceptive emails or messages that appear to come from credible sources, prompting the victim to take action, such as clicking on a malicious link or providing personal information. In the context of cybersecurity, recognizing phishing as a social engineering attack emphasizes the importance of user awareness and training. Attackers craft their messages to evoke trust and urgency, making it crucial for individuals to verify the authenticity of requests for information before responding. This highlights the ongoing need for security measures that combine technology with human vigilance to defend against such threats.

SAMPLE

7. What is Active Directory?

A. A web-based application for managing files

B. A directory service for Windows domain networks

C. A type of virtual private network

D. A security protocol for user authentication

Active Directory is primarily recognized as a directory service for Windows domain networks. It plays a crucial role in managing and organizing network resources such as users, computers, and security policies within a Windows environment. By serving as a centralized database, it enables administrators to efficiently manage identity and access services, authenticate users and devices, and enforce security policies across the organization. In contrast, the other options define concepts that do not encompass the full scope of Active Directory's functionalities. A web-based application for managing files does not reflect the functionality of a directory service, as it typically refers to content management rather than user and resource management. A virtual private network (VPN) is specifically focused on securely connecting users over the internet rather than managing directory services. Meanwhile, a security protocol for user authentication is a narrower concept that deals with the processes through which identities are verified, which is just one aspect of what Active Directory accomplishes. Therefore, interpreting Active Directory as a directory service accurately captures its essence as a foundational element of network management within Windows domains.

8. Which type of digital footprint is created automatically without user intent?

A. Active digital footprint

B. Passive digital footprint

C. Private digital footprint

D. Public digital footprint

A passive digital footprint is created automatically without user intent. This type of footprint is formed when a user's activities are tracked or recorded by third-party services without their direct engagement. Examples include website cookies, IP address tracking, and metadata collection from online interactions. Since users are often unaware of these automated processes, it highlights how their online presence can be shaped by interactions that they did not deliberately initiate. Active digital footprints, in contrast, consist of traces that users intentionally leave behind while interacting with online platforms, such as posting on social media or creating accounts. Private digital footprints refer to the information that users wish to keep concealed or restricted in access. Public digital footprints encompass all information that is openly available to anyone online, often derived from both active and passive interactions but can still include user-initiated actions. The distinction lies primarily in the level of user agency in creating the footprint.

SAMPLE

9. What is the ultimate goal of a security policy in an organization?

A. To dictate employee behavior

B. To outline compliance measures

C. To safeguard organizational assets

D. To limit network access

The ultimate goal of a security policy in an organization is to safeguard organizational assets. This encompasses protecting not just the physical resources, such as hardware and infrastructure, but also the intangible assets, including sensitive data and intellectual property. By establishing a clear framework of guidelines and practices, a security policy creates a foundation for risk management and helps ensure that assets are shielded from threats and vulnerabilities. It is designed to promote a culture of security awareness among employees, facilitate compliance with relevant laws and regulations, and ultimately protect the organization's reputation, financial stability, and operational integrity. The other options might reflect important components of a security policy, but they serve more as means to achieve the overarching goal of asset protection.

10. What type of system is primarily concerned with detecting and responding to breaches?

A. An Intrusion Prevention System (IPS)

B. An Intrusion Detection System (IDS)

C. A Data Loss Prevention System (DLP)

D. A Security Information and Event Management system (SIEM)

An Intrusion Detection System (IDS) is designed specifically to monitor network or system activities for malicious activities or policy violations. The primary function of an IDS is to identify potential breaches by analyzing traffic and logs. When a threat is detected, the IDS can either notify administrators or take predefined actions based on the severity of the threat. While an IPS also addresses breaches, its main role is to actively prevent them by blocking malicious traffic in real-time. In contrast, the focus of an IDS is on detection and alerting rather than proactive prevention. A Data Loss Prevention (DLP) system is oriented towards preventing sensitive data from being lost, misused, or accessed by unauthorized users. It controls data movements and actions pertaining to sensitive information but does not specifically detect breaches in the same manner as an IDS. A Security Information and Event Management (SIEM) system consolidates and analyzes security events from various sources to provide a comprehensive overview of an organization's security posture. It excels at correlating logs and providing insights about security events, but its main purpose is not solely detecting breaches. Given this context, the essence of an IDS lies in its dedicated approach to monitoring, identifying, and alerting on potential breaches, making it the most suitable answer for the question posed

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://securityfundamentalsprofessionalcertification.examzify.com

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

SAMPLE