SECURITY FUNDAMENTALS PROFESSIONAL CERTIFICATION (SFPC) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

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 of the following is a widely recognized framework for managing cybersecurity risks?**

   A. CIS Controls

   B. SANS Institute Guidelines

   C. NIST Cybersecurity Framework

   D. ISO 27001 Standards

2. **What does HTTPS stand for?**

   A. HyperText Transfer Protocol Secure

   B. High Transfer Protocol Standard

   C. HyperText Transmission Protocol Service

   D. Hyper Transfer Protocol Secure

3. **What is the purpose of the Controlled Access Program Coordination (CAPCO) register?**

   A. To identify the categories, types, and levels of Special Access Programs (SAPs)

   B. To define the authorities for classifying, declassifying, and regrading sensitive documents

   C. To identify the official classification and control markings, and their authorized abbreviations and portion markings

   D. To define the requirements, restrictions, and measures necessary to safeguard classified information from unauthorized disclosure

4. **What is a key goal of information assurance?**

   A. To eliminate the need for secure systems

   B. To ensure the confidentiality, integrity, and availability of information

   C. To restrict access to information at all times

   D. To increase the volume of data handled

5. **When providing access to Social Media sites, what is NOT a requirement for the DoD agency?**

   A. Protection against malware

   B. Blocked access to prohibited content

   C. Individual compliance with ethics guidelines

   D. Constant monitoring for inappropriate access

SAMPLE

6. What is the primary objective of risk management in information security?

A. To ensure data is accessible at all times

B. To identify, assess, and mitigate risks to information assets

C. To enhance user satisfaction and trust

D. To eliminate all potential threats

7. What is the role of the government contracting activity when an uncleared contractor wishes to bid on a classified RFP?

A. Reject the contractor's bid formally

B. Ask the contractor to submit a sponsorship request to DSS

C. Sponsor the contractor for a facility security clearance

D. Ensure all owners of the contractor are U.S. citizens

8. What is an example of a preventive security control?

A. Intrusion detection systems

B. Firewalls

C. Security audits

D. Incident response plans

9. What key aspect does the principle of least privilege emphasize?

A. Access to all systems

B. Minimum necessary access for job functions

C. Shared access among all users

D. Access based on seniority

10. 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

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which of the following is a widely recognized framework for managing cybersecurity risks?

A. CIS Controls

B. SANS Institute Guidelines

C. NIST Cybersecurity Framework

D. ISO 27001 Standards

The NIST Cybersecurity Framework is considered a widely recognized framework for managing cybersecurity risks because it provides a structured approach to addressing and managing cybersecurity risks in a way that is aligned with business objectives. Developed by the National Institute of Standards and Technology (NIST), the framework emphasizes the importance of understanding organizational risks and integrating them into overall risk management practices. Key aspects of the NIST Cybersecurity Framework include its core functions—Identify, Protect, Detect, Respond, and Recover—which guide organizations in assessing their current posture, implementing effective security measures, and establishing a continuous improvement process. This framework is highly flexible, scalable, and applicable across various sectors, making it accessible for organizations of different sizes and industries. While other options like the CIS Controls, SANS Institute Guidelines, and ISO 27001 Standards provide valuable guidance in cybersecurity practices, they may focus on specific aspects or frameworks that do not encompass the broader, risk management-oriented approach that the NIST Cybersecurity Framework offers.

2. What does HTTPS stand for?

A. HyperText Transfer Protocol Secure

B. High Transfer Protocol Standard

C. HyperText Transmission Protocol Service

D. Hyper Transfer Protocol Secure

HTTPS stands for HyperText Transfer Protocol Secure. It is an extension of HTTP and is designed to provide a secure communication channel over a computer network. The 'S' at the end signifies that the data exchanged between the client (usually a web browser) and the server is encrypted, typically utilizing protocols such as SSL (Secure Sockets Layer) or TLS (Transport Layer Security). This encryption is crucial in ensuring the confidentiality and integrity of data, making HTTPS essential for protecting sensitive information such as passwords, credit card numbers, and personal data from potential attacks and eavesdropping. The other options are not correct as they either misrepresent the secure aspect of HTTP or do not represent a valid protocol associated with web security. For example, "High Transfer Protocol Standard" and "HyperText Transmission Protocol Service" do not exist in networking terminology, and "Hyper Transfer Protocol Secure" does not accurately describe the established protocol structure. Thus, the only accurate representation of HTTPS is HyperText Transfer Protocol Secure.

SAMPLE

3. What is the purpose of the Controlled Access Program Coordination (CAPCO) register?

A. To identify the categories, types, and levels of Special Access Programs (SAPs)

B. To define the authorities for classifying, declassifying, and regrading sensitive documents

C. To identify the official classification and control markings, and their authorized abbreviations and portion markings

D. To define the requirements, restrictions, and measures necessary to safeguard classified information from unauthorized disclosure

The Controlled Access Program Coordination (CAPCO) register serves a crucial role in the management of classified information by providing a structured approach to the identification of official classification and control markings. This is vital for ensuring that sensitive information is properly labeled, which facilitates its handling, storage, and dissemination. By identifying the specific classification levels, control markings, abbreviations, and portion markings, the CAPCO register helps personnel understand how to manage classified information appropriately—ensuring that those accessing the information can easily recognize its status and handling requirements. This systematic labeling is essential for maintaining the integrity and security of the information being managed. The other options, while relevant to the broader context of data classification and security, do not specifically capture the essence of the CAPCO register's purpose and function as it pertains to classification and control markings. Understanding the role of the CAPCO register is critical for anyone involved in handling classified materials, as it sets the groundwork for ensuring compliance with established security protocols.

4. What is a key goal of information assurance?

A. To eliminate the need for secure systems

B. To ensure the confidentiality, integrity, and availability of information

C. To restrict access to information at all times

D. To increase the volume of data handled

A key goal of information assurance is to ensure the confidentiality, integrity, and availability of information, which are collectively known as the CIA triad. This triad is fundamental in establishing a comprehensive framework for managing and protecting sensitive data. Confidentiality ensures that sensitive information is accessible only to those authorized to have access, protecting it from unauthorized disclosure. Integrity involves maintaining the accuracy and completeness of information, ensuring that data is not altered or destroyed in an unauthorized manner. Availability ensures that information is accessible to authorized users when needed, thus supporting operations and decision-making processes. By focusing on these three aspects, information assurance aims to create a secure environment that safeguards data from various threats while enabling legitimate users to access the necessary information without hindrance. This approach is fundamental in addressing the risks associated with information systems and helps organizations maintain trust and compliance with regulatory requirements. The other options do not align with the established goals of information assurance. For instance, eliminating the need for secure systems runs contrary to the fundamental principles of security, as it fails to recognize the inherent risks that information systems face. Restricting access to information at all times may hinder legitimate business processes and does not support the necessary availability of information. Lastly, simply increasing the volume of data handled does not

SAMPLE

5. When providing access to Social Media sites, what is NOT a requirement for the DoD agency?

A. Protection against malware

B. Blocked access to prohibited content

C. Individual compliance with ethics guidelines

D. Constant monitoring for inappropriate access

The requirement regarding constant monitoring for inappropriate access is viewed as a less formal necessity compared to the other options. While the Department of Defense (DoD) emphasizes security and compliance, constant active monitoring may not be specifically mandated within the guidelines for accessing social media sites. Instead, agencies typically focus on establishing protective measures like malware protection, content filtering, and ensuring individual ethical compliance. Protection against malware is crucial to safeguard the integrity of systems and data when accessing external websites. Blocking access to prohibited content helps maintain adherence to regulations and operational security. Individual compliance with ethics guidelines ensures that personnel use social media responsibly and in accordance with organizational values. These requirements uniquely pertain to maintaining security and ethical standards, making constant monitoring a secondary concern rather than a direct requirement.

6. What is the primary objective of risk management in information security?

A. To ensure data is accessible at all times

B. To identify, assess, and mitigate risks to information assets

C. To enhance user satisfaction and trust

D. To eliminate all potential threats

The primary objective of risk management in information security is to identify, assess, and mitigate risks to information assets. This involves a systematic process where organizations evaluate the potential risks that could impact their information systems and data, determining the likelihood and consequence of various threats. By understanding these risks, organizations can implement appropriate controls and strategies to limit the potential impact of these threats on their information assets. Effective risk management not only helps in protecting sensitive data but also ensures compliance with legal and regulatory requirements, supports business continuity, and enhances the overall security posture of the organization. It recognizes that while it may not be possible to eliminate all risks, proactive identification and mitigation of those risks are essential for safeguarding valuable information resources. Other options, while relevant to information security, do not encapsulate the comprehensive objective of risk management. Ensuring data accessibility, enhancing user satisfaction, and eliminating all potential threats, while important in their own contexts, do not directly address the structured approach to understanding and managing risks that is fundamental to effective risk management practices.

SAMPLE

7. What is the role of the government contracting activity when an uncleared contractor wishes to bid on a classified RFP?

A. Reject the contractor's bid formally

B. Ask the contractor to submit a sponsorship request to DSS

C. Sponsor the contractor for a facility security clearance

D. Ensure all owners of the contractor are U.S. citizens

In the context of government contracting with uncleared contractors wishing to bid on classified requests for proposals (RFPs), the correct answer highlights the role of the government contracting activity in facilitating the security clearance process. When an uncleared contractor is interested in bidding, the government has a vested interest in ensuring that necessary security measures are in place to protect sensitive information related to national security. Sponsoring the contractor for a facility security clearance signifies that the government recognizes the contractor's potential role in handling classified information and is willing to assist in the process of obtaining the appropriate clearances. The facility security clearance is essential for the contractor to comply with the requirements of the classified RFP and to engage in sensitive work for the government. The other options touch on different aspects of the clearance process but do not encapsulate the primary action expected from the contracting activity. Rejecting the bid outright would not align with encouraging competition and innovation from various contractors. Requesting a sponsorship from the Defense Security Service (DSS) is a procedural step, but the contracting activity itself is responsible for interface and communication with the contractor during this phase. Ensuring all owners are U.S. citizens is a requirement, but it's typically part of the security clearance process, rather than a direct action

8. What is an example of a preventive security control?

A. Intrusion detection systems

B. Firewalls

C. Security audits

D. Incident response plans

A firewall serves as an example of a preventive security control because its primary function is to restrict unauthorized access to or from a network. It does this by applying a set of defined rules for incoming and outgoing traffic, effectively creating a barrier between trusted internal networks and untrusted external networks. By monitoring and controlling this traffic, firewalls help prevent potential security breaches before they occur, thereby mitigating the risk of data loss or compromise. In the context of security controls, preventive measures are designed to stop incidents before they happen, rather than responding to them after they have occurred. This distinguishes preventive controls like firewalls from other options, such as intrusion detection systems, which primarily detect and alert on suspicious activity rather than prevent it, and security audits, which evaluate existing security measures but do not actively prevent incidents. Incident response plans also fall under the category of reactive measures, as they provide a structured approach to responding to security incidents once they have been detected.

SAMPLE

9. What key aspect does the principle of least privilege emphasize?

A. Access to all systems

B. Minimum necessary access for job functions

C. Shared access among all users

D. Access based on seniority

The principle of least privilege emphasizes providing users and systems with the minimum necessary access rights to perform their job functions. This means that individuals are granted only the permissions essential for them to carry out their responsibilities, reducing the risk of unauthorized access and potential security breaches. By limiting access, organizations can minimize the damage that could result from accidents or malicious actions, thereby enhancing overall security. This principle is foundational in information security practices, as it helps to prevent excessive permissions that could lead to vulnerabilities. For example, if an employee needs access to only specific data to do their job, granting them broader access would expose the system to unnecessary risks. By enforcing minimum necessary access, companies not only protect sensitive information but also create a clearer audit trail of who accessed what data and when, which is essential for compliance and monitoring.

10. 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.

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