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

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Table of Contents

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.

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!

Questions

1. **Which of the following is not considered when making a security clearance eligibility determination?**
   - **A. Education Level**
   - **B. Alcohol consumption**
   - **C. Financial considerations**
   - **D. Psychological Conditions**

2. **In information security, what does "vulnerability" refer to?**
   - **A. A solution to a potential threat**
   - **B. A weakness in a system that can be exploited**
   - **C. A method for securing sensitive information**
   - **D. A type of security software**

3. **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)**

4. **What is a security breach?**
   - **A. Any event in which stored data is lost**
   - **B. An incident where unauthorized access or disclosure of data occurs**
   - **C. A routine audit of security measures**
   - **D. A failure to update software and systems**

5. **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**

6. What is the main purpose of the principle of separation of duties?

A. To increase the efficiency of operations

B. To ensure compliance with legal standards

C. To prevent fraud and errors

D. To enhance employee productivity

7. Why would an organization use a firewall?

A. To connect different networks

B. To increase employee morale

C. To monitor and control incoming and outgoing traffic

D. To enable remote access

8. Which example best describes a security violation rather than a security infraction?

A. Printing classified documents in an open area

B. Putting classified documents in the wrong folder

C. Accidentally reviewing classified materials with unclassified documents

D. Not reporting a known security breach

9. How is a "distributed denial of service" (DDoS) attack characterized?

A. An attack targeting multiple networks only

B. Using a single source to disrupt service

C. Using multiple systems to overwhelm a target system

D. A security check on all incoming traffic

10. 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

Answers

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

Explanations

1. Which of the following is not considered when making a security clearance eligibility determination?

A. Education Level

B. Alcohol consumption

C. Financial considerations

D. Psychological Conditions

When making a security clearance eligibility determination, the decision is primarily based on how an individual's behavior, reliability, and trustworthiness reflect upon their responsibilities regarding sensitive information. Education level is not typically considered a direct factor in eligibility for security clearance. While a certain level of education might be a requirement for specific positions, it does not inherently influence the assessment of an individual's risk to national security or their ability to handle classified information. On the other hand, factors such as alcohol consumption, financial considerations, and psychological conditions are critical in evaluating an individual's overall stability and potential risk factor. These areas can reveal patterns of behavior that may suggest a vulnerability to coercion, susceptibility to illegal activity, or an inability to effectively manage the responsibilities associated with access to sensitive information. Thus, psychological evaluations, financial history reviews, and substance use assessments are all integral components of the clearance process, but educational qualifications do not play the same significant role in this context.

2. In information security, what does "vulnerability" refer to?

A. A solution to a potential threat

B. A weakness in a system that can be exploited

C. A method for securing sensitive information

D. A type of security software

In information security, "vulnerability" refers to a weakness in a system that can be exploited. This concept is fundamental because vulnerabilities can arise in various forms, such as software bugs, misconfigurations, or overlooked security measures, which attackers might leverage to gain unauthorized access or compromise the integrity of the system. Understanding vulnerabilities is critical for organizations to assess their security posture and implement measures to mitigate risks. By identifying and addressing these weaknesses, organizations can better protect their assets and sensitive information from potential threats. Other options reflect concepts associated with security but do not accurately define what a vulnerability is. Solutions to threats, methods for securing information, and types of security software are all important elements of information security strategy but do not specifically characterize the concept of vulnerability itself.

3. 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

4. What is a security breach?

A. Any event in which stored data is lost

B. An incident where unauthorized access or disclosure of data occurs

C. A routine audit of security measures

D. A failure to update software and systems

A security breach is fundamentally defined as an incident where unauthorized access or disclosure of data occurs. This encompasses a variety of scenarios, including situations where malicious actors gain access to sensitive information without permission or where data is inadvertently exposed to unauthorized individuals. Such breaches can have severe implications, ranging from identity theft and financial loss to reputational damage for organizations. The option concerning stored data being lost does not fully capture the essence of a security breach since loss of data does not inherently imply unauthorized access. Similarly, a routine audit of security measures is a proactive measure taken to strengthen security and prevent breaches, rather than an incident of a breach itself. Lastly, while a failure to update software and systems may indeed heighten security risks and vulnerabilities, it is not classified as a breach unless actual unauthorized access has taken place. Thus, the second option aligns precisely with the widely accepted definition of a security breach, emphasizing the aspect of unauthorized access or disclosure.

5. 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

6. What is the main purpose of the principle of separation of duties?

A. To increase the efficiency of operations

B. To ensure compliance with legal standards

C. To prevent fraud and errors

D. To enhance employee productivity

The principle of separation of duties is primarily aimed at preventing fraud and errors. This concept is critical in security and internal control systems, as it involves distributing responsibilities and tasks among different individuals or groups to create checks and balances. By ensuring that no single individual has control over all aspects of a financial transaction or critical operation, the risk of fraudulent activities, such as embezzlement or unauthorized actions, is significantly reduced. Furthermore, this division helps to catch and correct mistakes, as multiple people need to be involved in oversight and reviews. While increasing operational efficiency, ensuring compliance with legal standards, and enhancing employee productivity may be positive outcomes of implementing separation of duties, these are not the main focus of this principle. The primary goal remains to mitigate risks associated with fraud and inaccuracies, thus maintaining the integrity of processes within an organization.

7. Why would an organization use a firewall?

A. To connect different networks

B. To increase employee morale

C. To monitor and control incoming and outgoing traffic

D. To enable remote access

An organization would use a firewall primarily to monitor and control incoming and outgoing network traffic based on predetermined security rules. Firewalls serve as a barrier between a trusted internal network and untrusted external networks, such as the internet. This is crucial for protecting sensitive data and preventing unauthorized access to the organization's network resources. Firewalls inspect packets of data that are transmitted across the network and enforce security policies by allowing or blocking traffic based on specific criteria, such as IP addresses, protocols, and ports. This control helps prevent cyberattacks, including malware infections, unauthorized access, and data breaches, thereby safeguarding the organization's information and infrastructure. While it is possible for a firewall to serve additional functions, such as providing remote access or facilitating network connections, its primary purpose is centered on traffic management and security enforcement. This is why the correct answer emphasizes the role of a firewall in monitoring and controlling traffic.

8. Which example best describes a security violation rather than a security infraction?

A. Printing classified documents in an open area

B. Putting classified documents in the wrong folder

C. Accidentally reviewing classified materials with unclassified documents

D. Not reporting a known security breach

The situation that best exemplifies a security violation is the accidental review of classified materials alongside unclassified documents. A security violation typically involves a breach of established security protocols or regulations that compromises the integrity, confidentiality, or availability of sensitive information. In this case, reviewing classified materials in an inappropriate context, such as in the presence of unassigned individuals or unauthorized personnel, poses a direct risk to the safeguarding of that classified information. It surpasses the realm of minor errors or lapses in judgment typically observed in infractions. In contrast, while options like printing classified documents in an open area and putting classified documents in the wrong folder may represent significant lapses in security protocols, they are generally regarded as infractions due to the absence of malicious intent or a clear breach of security rules that directly compromises the information being handled. Not reporting a known security breach also indicates a failure to follow proper procedures but is more about neglecting the responsibility rather than an active manipulation or exposure of sensitive materials. Therefore, the act of reviewing classified materials accidentally with unclassified ones stands out as the scenario most indicative of a bona fide security violation.

9. How is a “distributed denial of service” (DDoS) attack characterized?

A. An attack targeting multiple networks only

B. Using a single source to disrupt service

C. Using multiple systems to overwhelm a target system

D. A security check on all incoming traffic

A distributed denial of service (DDoS) attack is characterized by the use of multiple systems to overwhelm a target system. This form of attack involves a network of compromised computers, often referred to as a botnet, that simultaneously send a flood of traffic to a single target. The intention is to exhaust the target's resources, such as bandwidth, memory, or processing power, which can effectively render the service unavailable to legitimate users. The nature of DDoS attacks, drawing on various sources to launch coordinated assaults, significantly amplifies their impact compared to single-source attacks. Because the incoming requests come from various locations, it becomes incredibly challenging for the target to distinguish between legitimate traffic and attack traffic or to effectively mitigate the assault. Understanding this characteristic of DDoS attacks is crucial for recognizing how such threats can severely disrupt services and underscores the importance of robust network security measures to defend against them.

10. 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.

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!