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

STUDY GUIDE

Prepare with structure. Pass with confidence

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. **What does the security professional do during the "Award Contract" step of the contracting process?**

   A. Ensure classification level for the bid is appropriate

   B. Interface with the Cognizant Security Organization

   C. Ensure contractors follow safeguarding guidance

   D. Review specific security requirements with the contracting officer

2. **In access control, what does the term "least privilege" mean?**

   A. Allowing users maximum access for flexibility

   B. Granting users the minimum access necessary for their tasks

   C. Enabling users to access all resources freely

   D. Limiting access based on user preferences

3. **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

4. **What is the primary distinction between qualitative and quantitative risk assessment?**

   A. Qualitative uses numerical values, while quantitative uses subjective judgment

   B. Quantitative uses numerical values, while qualitative uses subjective judgment

   C. Both methods use subjective judgment but differ in their application

   D. Qualitative focuses solely on compliance, while quantitative focuses on risk

5. **What does the term "phishing" refer to in cybersecurity?**

   A. A legitimate method to collect user information

   B. A technique to protect against identity theft

   C. A fraudulent attempt to obtain sensitive information

   D. A strategy used for network penetration testing

6. What is the role of the National Institute of Standards and Technology (NIST) in cybersecurity?

A. To provide entertainment in technology

B. To develop standards and guidelines for managing cybersecurity risk

C. To enforce laws against cybercrime

D. To promote internet technologies

7. Which of the following strategies can help secure your digital footprint?

A. Using the same password for all accounts

B. Regularly changing privacy settings on social media

C. Enabling location services at all times

D. Ignoring updates and security patches

8. A position designated as a DoD noncritical-sensitive civilian position may fall under any of the following criteria, EXCEPT?

A. A position not requiring eligibility for access to classified information, but having the potential to cause significant or serious damage to the national security.

B. A position requiring eligibility for access to Top Secret information.

C. A position requiring eligibility for access to confidential information.

D. A position requiring eligibility for access to secret information.

9. Which type of Special Access Program (SAP) protects sensitive research and development activities?

A. Research and Technology SAP

B. Operations and Support SAP

C. Acquisition SAP

D. Intelligence SAP

10. How can organizations ensure the effectiveness of their security measures?

A. By avoiding regular assessments

B. By conducting continuous evaluations and updates

C. By ignoring user feedback

D. By reinforcing previous policies without changes

Answers

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

Explanations

1. What does the security professional do during the "Award Contract" step of the contracting process?

A. Ensure classification level for the bid is appropriate

B. Interface with the Cognizant Security Organization

C. Ensure contractors follow safeguarding guidance

D. Review specific security requirements with the contracting officer

During the "Award Contract" step of the contracting process, reviewing specific security requirements with the contracting officer is crucial because it ensures that all security concerns are adequately addressed before the contract is finalized. This review helps to align the expectations and responsibilities regarding security measures between the contracting parties. Effective communication of security requirements at this stage helps to mitigate potential risks and enhances the overall security posture of the project. It also guarantees that the awarded contractor understands their obligations related to security compliance, protection of sensitive information, and any specific safeguarding measures that must be implemented throughout the duration of the contract. This proactive step is key to maintaining a secure environment and ensuring that contract conditions support the organization's security objectives. The other options, while relevant to different aspects of security in the contracting process, do not specifically address the critical interaction that occurs during the awarding of the contract itself.

2. In access control, what does the term "least privilege" mean?

A. Allowing users maximum access for flexibility

B. Granting users the minimum access necessary for their tasks

C. Enabling users to access all resources freely

D. Limiting access based on user preferences

The principle of "least privilege" is a fundamental concept in access control and information security. It refers to the practice of granting users the minimum level of access—or permissions—necessary for them to perform their specific tasks or responsibilities. This means that users should have only the permissions required to complete their job functions and nothing more. Implementing least privilege helps to reduce the risk of accidental or malicious misuse of sensitive data or systems. For example, if a user does not require administrative privileges to perform their tasks, they should not be granted those privileges. This minimizes the attack surface and decreases the potential for security breaches, as fewer privileges mean reduced risk of exploitation by attackers or even the users themselves, whether intentionally or unintentionally. By restricting access in this way, organizations can better protect their assets, comply with regulatory requirements, and enhance overall security posture. Therefore, the correct understanding of "least privilege" is crucial for effective access control and risk management strategies.

3. 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.

4. What is the primary distinction between qualitative and quantitative risk assessment?

A. Qualitative uses numerical values, while quantitative uses subjective judgment

B. Quantitative uses numerical values, while qualitative uses subjective judgment

C. Both methods use subjective judgment but differ in their application

D. Qualitative focuses solely on compliance, while quantitative focuses on risk

The primary distinction between qualitative and quantitative risk assessment lies in their methodologies and approaches to assessing risk. In a quantitative risk assessment, numerical values are assigned to potential risks, often using statistical data, metrics, or established risk calculations. This approach enables organizations to calculate the likelihood of risk events occurring and their potential impacts in numerical terms, allowing for a more objective analysis that can be more easily communicated through figures and percentages. On the other hand, qualitative risk assessment relies on subjective judgment to evaluate risks based on opinion, experience, or expert assessment. This method often involves categorizing risks into levels of impact or likelihood without numerical quantification. Qualitative assessments may include descriptive scales, such as low, medium, and high, for the evaluation of risks and their consequences. This approach is particularly useful when data is limited or when a more nuanced understanding of the risks is necessary. Understanding this distinction is crucial for selecting the appropriate risk assessment method based on the organization's needs, available data, and the context of the risks being evaluated.

5. What does the term "phishing" refer to in cybersecurity?

A. A legitimate method to collect user information

B. A technique to protect against identity theft

C. A fraudulent attempt to obtain sensitive information

D. A strategy used for network penetration testing

Phishing refers to a fraudulent attempt to obtain sensitive information, such as usernames, passwords, credit card details, and other personal data, by disguising as a trustworthy entity in electronic communications. This typically occurs through deceptive emails or websites that appear legitimate, enticing individuals to share their information. The tactic exploits the human tendency to trust what seems familiar, leading victims to unknowingly give away vital information that can be misused for identity theft or fraud. Understanding the mechanics of phishing is crucial for cybersecurity awareness, as it highlights the importance of vigilance and skepticism when encountering unsolicited messages or requests for sensitive information. Cybersecurity training often emphasizes recognizing the signs of phishing attempts to help individuals avoid these traps. This is why C is the correct interpretation of the term in the context of cybersecurity.

6. What is the role of the National Institute of Standards and Technology (NIST) in cybersecurity?

A. To provide entertainment in technology

B. To develop standards and guidelines for managing cybersecurity risk

C. To enforce laws against cybercrime

D. To promote internet technologies

The National Institute of Standards and Technology (NIST) plays a crucial role in cybersecurity by developing standards and guidelines for managing cybersecurity risks. This involves creating frameworks, guidelines, and best practices that organizations can adopt to enhance their security posture and ensure compliance with relevant regulations. NIST's primary focus is to provide a structured approach to cybersecurity that organizations of all sizes can implement. By creating publications such as the NIST Cybersecurity Framework, NIST helps organizations identify, protect, detect, respond, and recover from cybersecurity incidents. This framework is designed to be flexible and accessible, allowing organizations to tailor it to their specific needs and risk profiles. Furthermore, NIST collaborates with various stakeholders, including industry leaders, academia, and government agencies, to promote an integrated risk management approach. This collaboration ensures that the standards and guidelines are comprehensive, relevant, and effective in addressing evolving cybersecurity threats. In contrast to other roles mentioned in the options, NIST does not enforce laws against cybercrime, promote internet technologies, or provide entertainment. Its function is distinctly centered around establishing a secure foundation for managing cybersecurity risks through well-defined standards and practices.

7. Which of the following strategies can help secure your digital footprint?

A. Using the same password for all accounts

B. Regularly changing privacy settings on social media

C. Enabling location services at all times

D. Ignoring updates and security patches

Regularly changing privacy settings on social media is a proactive strategy to help secure your digital footprint. Social media platforms frequently update their privacy policies and settings. By regularly reviewing and adjusting these settings, you can control what personal information is visible to others and to what extent. This habit ensures that you are leveraging the latest privacy features and protections, thus minimizing the risk of unwanted exposure or data breaches. Maintaining up-to-date privacy settings can also help in managing who can see your posts, who can contact you, and how your information is shared with third parties. This ongoing practice is essential for safeguarding your personal data and maintaining your online privacy in a landscape where threats can evolve rapidly. The other strategies mentioned do not support improved security and can lead to vulnerabilities. Using the same password across multiple accounts increases the risk of a single breach leading to access to numerous accounts. Enabling location services at all times can unintentionally share your location information with anyone who accesses your social media. Ignoring updates and security patches leaves your systems vulnerable to known exploits and threats.

8. A position designated as a DoD noncritical-sensitive civilian position may fall under any of the following criteria, EXCEPT?

A. A position not requiring eligibility for access to classified information, but having the potential to cause significant or serious damage to the national security.

B. A position requiring eligibility for access to Top Secret information.

C. A position requiring eligibility for access to confidential information.

D. A position requiring eligibility for access to secret information.

The designation of a position as DoD noncritical-sensitive is primarily concerned with the level of access required for that position concerning classified information. In this context, a position that requires eligibility for access to Top Secret information is not classified as noncritical-sensitive because such positions are typically regarded as critical-sensitive due to the significant impact their access could have on national security. Positions that may fall under the noncritical-sensitive category include those that do not require access to classified information (or require access to lower classification levels) but still hold the potential to impact national security. Therefore, options that reference access to Confidential or Secret information are appropriate within the noncritical-sensitive category, as they do not involve the highest level of sensitivity associated with Top Secret access.

9. Which type of Special Access Program (SAP) protects sensitive research and development activities?

A. Research and Technology SAP

B. Operations and Support SAP

C. Acquisition SAP

D. Intelligence SAP

The correct answer, which pertains to the type of Special Access Program that aims to safeguard sensitive research and development activities, is associated with the Acquisition SAP. This category specifically focuses on the management and protection of classified information that is critical to the development and acquisition of defense systems and technologies. Research and development activities often fall under this umbrella, as they involve the creation and testing of new products that may have significant national security implications. Acquisition SAPs are designed to limit access to information related to pivotal projects and technologies that could be targeted by adversaries, thereby ensuring that sensitive information is handled in a secure manner throughout the lifecycle of the program. This includes everything from initial research to the final acquisition of systems and capabilities, thus supporting national defense objectives effectively. The other options relate to different aspects of Special Access Programs. Research and Technology SAP specifically addresses the protection of the development of new technologies but does not encompass the broader acquisition processes. Operations and Support SAP focuses on operational aspects and support systems rather than research and development. Intelligence SAP is geared toward intelligence operations and managing classified information concerning intelligence activities. Each of these serves a different purpose in securing sensitive information related to national security, distinguishing them from the role of the Acquisition SAP in protecting R&D activities.

10. How can organizations ensure the effectiveness of their security measures?

A. By avoiding regular assessments

B. By conducting continuous evaluations and updates

C. By ignoring user feedback

D. By reinforcing previous policies without changes

The effectiveness of security measures is best ensured through continuous evaluations and updates. This process involves regularly reviewing and testing existing security protocols, assessing potential vulnerabilities, and adapting to new threats as they arise. Continuous evaluations help organizations to identify any gaps in their security posture and to respond proactively to changes in the threat landscape, such as emerging cyber threats, changes in business operations, or evolving regulatory requirements. This approach fosters a culture of agility within the security team, enabling them to implement timely updates and enhancements to security measures. Furthermore, continuous evaluation entails involving various stakeholders, gathering data based on real-world events, and updating security policies and technologies to maintain an effective defense against risks. By adopting this proactive mindset, organizations can mitigate the chances of breaches and improve their overall security resilience. This approach contrasts sharply with the other choices, which advocate for avoidance of evaluation, neglect of feedback, or adherence to outdated policies, ultimately weakening an organization's security posture.

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!