Advanced Security Training (AST) Practice Test (Sample)

Study Guide

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 should be included in a social media policy for businesses?

A. Guidelines on posting personal opinions

B. Recommendations for password creation

C. Prohibited activities related to social media

D. Best practices for creating viral content

2. What does Section 11 of the SSR prohibit without authorization?

A. The use of electronic surveillance tools

B. The carrying or use of restraining devices

C. The employment of security workers

D. The registration of security businesses

3. What defines Passive Resistance?

A. Subject actively resists control by physical means

B. Subject complies with all SP requests

C. Subject does not actively assist but also does not resist physically

D. Subject attempts to escape the area

4. What responsibility do licensed security businesses have regarding their workers?

A. To monitor all worker movements

B. To ensure workers only use approved restraining devices

C. To provide ongoing training for all employees

D. To document every encounter

5. When a subject escalates to an Active Resister, how should they be treated?

A. As a Passive Resister

B. As Cooperative

C. As an Active Resister

D. With increased communication efforts

6. What does the Security Programs Division (SPD) signify?

- **A. A rebranding of existing security divisions**
- **B. A new division created for handling illegal activities**
- **C. A division solely focused on technology**
- **D. A temporary initiative for developing security policies**

7. What is the importance of maintaining a distance from subjects?

- **A. It reduces the chance of aggression**
- **B. It enhances verbal communication**
- **C. It ensures safety for all parties**
- **D. It complicates the situation**

8. What is NOT likely to improve when a Service Provider (SP) stands very close to subjects?

- **A. Reaction time**
- **B. Authority perception**
- **C. Communication effectiveness**
- **D. Subject compliance**

9. In the context of cybersecurity, what is a primary goal of a social media policy?

- **A. To increase social media followers**
- **B. To prevent misinformation**
- **C. To outline acceptable use to reduce security vulnerabilities**
- **D. To promote personal branding of employees**

10. What does patch management refer to?

- **A. The process of monitoring network traffic**
- **B. Identifying user access levels**
- **C. The process of managing updates and patches to software**
- **D. The scheduling of employee training sessions**

Answers

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

Explanations

1. Which of the following should be included in a social media policy for businesses?

A. Guidelines on posting personal opinions

B. Recommendations for password creation

C. Prohibited activities related to social media

D. Best practices for creating viral content

Including prohibited activities related to social media in a business's social media policy is essential for several reasons. It sets clear expectations for employees regarding what is considered acceptable and unacceptable behavior while representing the company online. This can help safeguard the company's reputation, protect sensitive information, and ensure compliance with legal and regulatory requirements. When businesses clearly outline prohibited activities, such as posting confidential information, engaging in harassment or cyberbullying, or making defamatory statements about colleagues or competitors, it helps mitigate risks associated with social media use. Employees will better understand the boundaries set forth by the organization and the potential consequences of violating these guidelines. Providing this guidance can help foster a responsible and respectful online presence, encouraging employees to represent their organization positively and avoid actions that could lead to disciplinary measures or damage to the organization's brand and credibility.

2. What does Section 11 of the SSR prohibit without authorization?

A. The use of electronic surveillance tools

B. The carrying or use of restraining devices

C. The employment of security workers

D. The registration of security businesses

Section 11 of the SSR, which stands for Security Services Regulation, specifically addresses the carrying or use of restraining devices without proper authorization. This is critical because restraining devices can have significant implications for personal safety and legal rights. They can be potentially harmful and may lead to misuse if individuals are not properly trained or authorized to use them. The regulation ensures that only qualified and authorized personnel are permitted to carry such devices, which helps mitigate risks to both the individuals being restrained and the security personnel themselves. This helps maintain a standardized level of professional accountability and safety in the security industry. The other options pertain to different aspects of security activities, but they do not specifically highlight the stringent controls on restraining devices that Section 11 addresses. The focus of this section is primarily on the potential risks and liabilities involved with using restraining devices, making authorization a crucial requirement.

3. What defines Passive Resistance?

A. Subject actively resists control by physical means

B. Subject complies with all SP requests

C. Subject does not actively assist but also does not resist physically

D. Subject attempts to escape the area

Passive resistance is characterized by a lack of active opposition or aggression from the subject. Instead of physically resisting or complying fully, the individual may not help the situation while also refraining from any form of physical confrontation or escape. This type of behavior can manifest in various contexts, indicating that while the individual is present and under some form of control, they choose to neither assist nor actively hinder the situation. The recognition of this form of resistance is crucial in settings like security and law enforcement, as it influences how personnel should approach the subject. Understanding that passive resistance does not involve physical force helps security professionals to communicate and manage the situation more effectively, reducing the risk of escalation.

4. What responsibility do licensed security businesses have regarding their workers?

A. To monitor all worker movements

B. To ensure workers only use approved restraining devices

C. To provide ongoing training for all employees

D. To document every encounter

Ensuring that workers only use approved restraining devices is a critical responsibility for licensed security businesses. This obligation stems from the need to maintain safety and compliance with legal standards. By restricting the use of restraining devices to those that have received proper approval, security businesses mitigate the risk of injury to both employees and individuals being restrained. Utilizing unapproved devices could lead to excessive force situations, legal liabilities, and could jeopardize the integrity and reputation of the security agency. In contrast, while monitoring worker movements, providing ongoing training, and documenting encounters are important components of a security business, they are not universally mandated responsibilities in the same way that the use of approved restraining devices is. Monitoring movements can be seen as an operational necessity, but it does not directly address the safety and compliance issues. Ongoing training is essential for skill enhancement and awareness, yet the objective of legal compliance and safety takes precedence in the use of restraining devices. Documenting encounters is important for accountability but does not directly relate to the operational safety concerns tied to the usage of such equipment. Thus, ensuring the use of approved restraining devices stands out as a clear and specific responsibility in the context of licensed security operations.

5. When a subject escalates to an Active Resister, how should they be treated?

A. As a Passive Resister

B. As Cooperative

C. As an Active Resister

D. With increased communication efforts

When a subject escalates to being classified as an Active Resister, it indicates that they are actively opposing or resisting directives being given by law enforcement or security personnel. This behavior requires a different approach than other classifications of resistive behavior, such as being a Passive Resister, where individuals may simply refuse to comply but do not pose an immediate threat. Treating the subject as an Active Resister means that appropriate measures must be taken to ensure the safety of all parties involved, including personnel and bystanders. This may involve a readiness to use physical intervention techniques or methods that are suitable for managing individuals who are not only non-compliant but are also exhibiting more aggressive or confrontational behaviors. The categorization dictates a proportional response that matches the level of resistance being encountered. In contrast, recognizing the subject as a Passive Resister or Cooperative would fail to address the potential risks involved when someone is actively resisting. Similarly, merely increasing communication efforts without acknowledging the level of resistance may not effectively neutralize the situation or ensure safety. Thus, identifying the subject as an Active Resister is crucial for determining the right tactical response and upholding effective security practices.

6. What does the Security Programs Division (SPD) signify?

A. A rebranding of existing security divisions

B. A new division created for handling illegal activities

C. A division solely focused on technology

D. A temporary initiative for developing security policies

The Security Programs Division (SPD) signifies a rebranding of existing security divisions. This means that the SPD represents an evolution or restructuring of how security functions are organized within an organization. The intention behind such a rebranding often includes aims to improve operational efficiency, integrate various security practices, and enhance communication across different security domains. Rebranding can help consolidate resources, unify different teams under a common mission, and potentially address any shortcomings observed in the previous structure. By creating a cohesive division like the SPD, organizations seek to foster a stronger approach to security concerns, emphasizing a comprehensive strategy rather than a fragmented one. Understanding the significance of this rebranding is critical as it reflects the organization's commitment to adapting to new security challenges and integrating best practices in a more streamlined manner.

7. What is the importance of maintaining a distance from subjects?

A. It reduces the chance of aggression

B. It enhances verbal communication

C. It ensures safety for all parties

D. It complicates the situation

Maintaining a distance from subjects is vital for ensuring safety for all parties involved. This practice serves several crucial functions in high-stress or potentially threatening situations. Firstly, it provides a physical buffer that can deter aggressive behavior, as individuals may feel less threatened when there is space between them. It also allows for better reaction time, enabling individuals to adjust quickly to any unforeseen actions from the subject. Moreover, maintaining distance can help create a calmer environment, which is beneficial for both the individual maintaining the distance and the subject. Those involved are often better equipped to think clearly and make rational decisions when there is a physical separation. This is particularly important in de-escalation strategies, where the goal is to diffuse tension and not escalate a situation further. While it can facilitate verbal communication, especially in minimizing misunderstandings that arise from personal space violations, the primary focus of maintaining distance centers around safety for everyone involved. This prioritization of safety makes it a critical aspect of training in various security-related fields.

8. What is NOT likely to improve when a Service Provider (SP) stands very close to subjects?

A. Reaction time

B. Authority perception

C. Communication effectiveness

D. Subject compliance

When a Service Provider (SP) stands very close to subjects, the improvement of various dynamics can vary based on proximity. Reaction time refers to how quickly a subject can respond to stimuli or commands. While being close may allow for quicker feedback or responses in some situations, it does not inherently enhance the speed at which individuals can process information or react. This can lead to the conclusion that standing close does not significantly impact reaction time in a positive way. On the other hand, authority perception, communication effectiveness, and subject compliance are all likely to be positively affected by proximity. When an SP is closer to subjects, it often enhances their authoritative presence, as individuals may perceive them as more commanding or engaged. Improved communication effectiveness can result from verbal and non-verbal cues that become clearer with reduced physical distance, facilitating better understanding. Lastly, closer proximity may lead to enhanced subject compliance as individuals may feel more compelled to follow instructions when the SP is physically nearby, which can create a sense of urgency or immediacy. This context illustrates why the option about reaction time stands out as the least likely to improve in this scenario.

9. In the context of cybersecurity, what is a primary goal of a social media policy?

A. To increase social media followers

B. To prevent misinformation

C. To outline acceptable use to reduce security vulnerabilities

D. To promote personal branding of employees

A primary goal of a social media policy is to outline acceptable use to reduce security vulnerabilities. Social media can be a significant vector for security threats, including data breaches, phishing, and reputation damage. By establishing guidelines for how employees should engage with social media, organizations can mitigate risks associated with unauthorized information sharing and improper account handling. This policy typically covers aspects such as what information can be shared, how to represent the organization online, and proper security practices for personal accounts that may relate to work. By clearly defining these parameters, a social media policy helps create a safer environment for both the organization and its employees, ultimately reducing the chances of cybersecurity incidents occurring through social platform interactions. The other options, while related to aspects of social media, do not directly reflect the core purpose of such a policy. Increasing followers, preventing misinformation, and promoting personal branding are important but serve different strategic objectives that may not directly address the need for security and acceptable use standards.

10. What does patch management refer to?

A. The process of monitoring network traffic

B. Identifying user access levels

C. The process of managing updates and patches to software

D. The scheduling of employee training sessions

Patch management refers to the process of managing updates and patches to software. This involves identifying, acquiring, installing, and verifying updates to ensure that software is up-to-date and secure. The purpose of patch management is to protect systems from vulnerabilities that could be exploited by attackers, thereby maintaining the integrity and security of the systems and data. By applying patches promptly, organizations can mitigate risks that arise from security vulnerabilities in software applications, operating systems, and other components. This process is essential for maintaining improved performance, fixing bugs, and addressing any issues that may compromise system functionality or security. Regular and systematic patch management helps organizations safeguard their infrastructure against threats and reduces the overall risk of security breaches, demonstrating its critical role in any comprehensive cybersecurity strategy.

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://advsecuritytraining.examzify.com

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