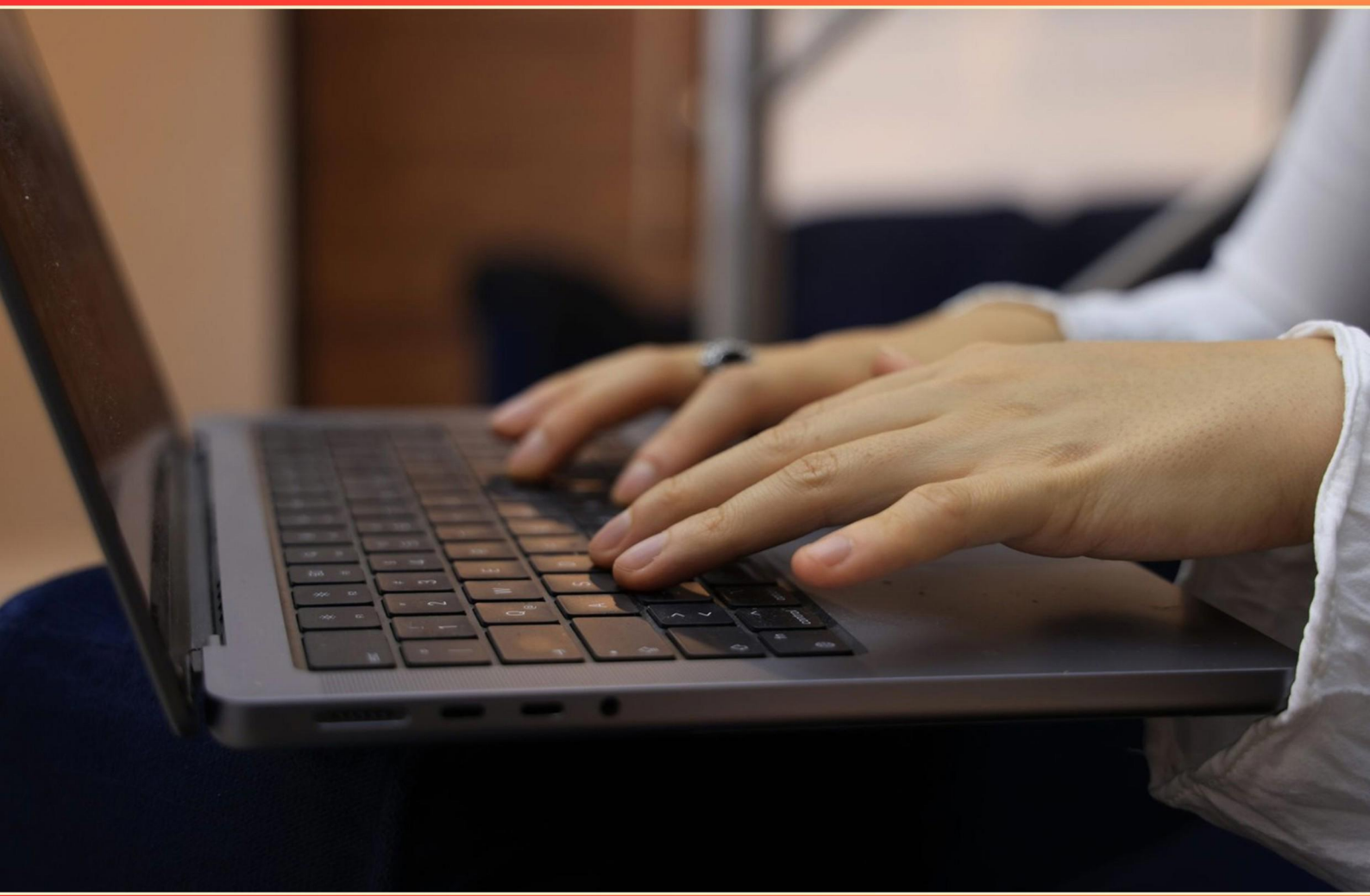
# ADVANCED SECURITY TRAINING (AST) PRACTICE TEST (SAMPLE)

## STUDY GUIDE



## SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE**

https://advsecuritytraining.examzify.com

# 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 framework is commonly used for incident response planning?**

A. ISO 27001 Framework

B. COBIT Framework

C. NIST Cybersecurity Framework

D. ITIL Framework

**2. Which term describes the use of more force than is reasonably necessary?**

A. Deadly force

B. Excessive force

C. Coercive force

D. Minimal force

**3. Which behavior indicates a cooperative subject?**

A. The subject displays aggression towards the SP

B. The subject ignores SP commands

C. The subject responds positively to SP's presence and direction

D. The subject engages in a vigorous struggle

**4. When must use of force reports be completed?**

A. Only when severe force is used

B. When a subject refuses to comply

C. Anytime a SP applies any kind of physical force to a subject

D. When the incident involves multiple officers

**5. What does continuity planning entail in security management?**

A. Preparing for software updates

B. Planning for the continuation of operations after a disruptive event

C. Designing new user interfaces for applications

D. Establishing marketing strategies

**6. What does "Security Awareness Training" focus on?**

A. Educating employees about security policies, practices, and the importance of security

B. Training IT staff on network configurations

C. Scheduling regular system updates and patches

D. Explaining legal responsibilities regarding data protection

**7. What term describes a subject that is compliant and agreeable with a security personnel?**

A. Cooperative

B. Compliant

C. Resistant

D. Nonchalant

**8. What is the primary goal of the Situational Assessment process?**

A. To find weaknesses in a team

B. To evaluate threats and dynamics

C. To generate reports on incidents

D. To train new personnel

**9. 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

**10. What does relative positioning refer to in the context of security personnel?**

A. The distance a subject maintains from the SP

B. The SP's location compared to the subject's

C. The emotional distance between the SP and the subject

D. The physical size of the SP relative to the subject

# Answers

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

# Explanations

## 1. Which framework is commonly used for incident response planning?

A. ISO 27001 Framework

B. COBIT Framework

C. NIST Cybersecurity Framework

D. ITIL Framework

*The NIST Cybersecurity Framework is widely recognized for incident response planning because it provides a structured approach to managing cybersecurity risks. This framework emphasizes five core functions: Identify, Protect, Detect, Respond, and Recover. Each of these functions guides organizations in establishing a comprehensive incident response strategy. Specifically, the Respond function is critical for incident management, as it outlines processes for planning, communication, analysis, mitigation, and improvements following an incident. By using the NIST framework, organizations can ensure that their incident response plans are aligned with best practices, thereby enhancing their resilience against cyber threats. Other frameworks like ISO 27001 focus on establishing an overall information security management system but are not primarily centered on incident response. COBIT is aligned more with governance and management of enterprise IT and doesn't provide specific guidance for incident response planning. ITIL, while it offers valuable service management practices, does not specifically target cybersecurity incident response yet can be integrated as a support process within an organization's incident response strategy. Thus, the NIST Cybersecurity Framework stands out as the best choice for incident response planning.*

## 2. Which term describes the use of more force than is reasonably necessary?

A. Deadly force

B. Excessive force

C. Coercive force

D. Minimal force

*The term that best describes the use of more force than is reasonably necessary is excessive force. This concept is critical in law enforcement and security contexts, as it pertains to the appropriate application of force in various situations. Excessive force typically arises when an officer or security personnel applies a level of physical force that is greater than what is deemed reasonable to accomplish a lawful purpose, such as detaining a suspect or protecting oneself. Understanding this term is essential because it reflects the balance between ensuring safety and upholding rights. When force is deemed excessive, it can lead to legal consequences, loss of trust in law enforcement, civil rights violations, and could ultimately endanger public safety. Recognizing the standards for reasonable force helps professionals navigate complex situations while maintaining accountability and ethical standards.*

## 3. Which behavior indicates a cooperative subject?

A. The subject displays aggression towards the SP

B. The subject ignores SP commands

C. The subject responds positively to SP's presence and direction

D. The subject engages in a vigorous struggle

*A behavior indicating a cooperative subject is one where the individual responds positively to the presence and direction of the security personnel (SP). This implies that the subject is willing to engage constructively and follow instructions, which is essential for effective communication and collaboration in any security scenario. When a subject exhibits this behavior, it demonstrates a level of respect, understanding, and compliance appropriate for a cooperative interaction. Such cooperation can significantly facilitate the situation, allowing for smoother operations and reducing the need for force or intense interventions. The cooperative nature of the subject ensures that the security personnel can carry out their duties more efficiently, as the subject is actively participating in the process rather than resisting or causing disruption.*

## 4. When must use of force reports be completed?

A. Only when severe force is used

B. When a subject refuses to comply

C. Anytime a SP applies any kind of physical force to a subject

D. When the incident involves multiple officers

*The requirement for completing use of force reports is grounded in the principles of accountability and transparency in law enforcement practices. When any type of physical force is applied to a subject, it is crucial for officers to document the circumstances surrounding the use of that force. This includes detailing the justification for its use, the actions of the individual involved, and the outcomes of the incident. This comprehensive documentation serves several key purposes. Firstly, it helps to ensure that officers are held accountable for their actions and decisions during confrontations. Secondly, it provides a record that can be reviewed for training and policy development, which is vital for improving de-escalation tactics and minimizing unnecessary force in the future. Lastly, thorough reporting contributes to public trust in law enforcement agencies by demonstrating a commitment to oversight and ethical practices. In contrast, the other scenarios mentioned may not encompass the full range of situations where a use of force report is warranted. For example, only reporting when severe force is applied could lead to inadequate documentation and oversight of less severe incidents that may still require scrutiny. Similarly, only requiring reports when a subject does not comply or when multiple officers are involved would overlook numerous incidents that merit detailed reporting, regardless of compliance levels or the number of officers involved.*

## 5. What does continuity planning entail in security management?

A. Preparing for software updates

B. Planning for the continuation of operations after a disruptive event

C. Designing new user interfaces for applications

D. Establishing marketing strategies

*Continuity planning in security management focuses primarily on ensuring that an organization can maintain essential functions and operations after experiencing disruptions, such as natural disasters, cyberattacks, or other crises. This involves identifying critical business functions, assessing risks, and developing strategies and procedures that enable an organization to respond effectively and recover quickly. By emphasizing the importance of planning for the continuation of operations, organizations can minimize downtime, safeguard important data, and protect their assets while ensuring that they can continue serving their stakeholders even in adverse circumstances. The other options do not align with the core objectives of continuity planning. Preparing for software updates pertains more to routine IT maintenance rather than crisis management. Designing new user interfaces is a task related to user experience and application development, not directly connected to operational resilience. Establishing marketing strategies involves promoting and selling products or services, which is not part of the continuity planning framework focused on operational sustainability during disruptions.*

## 6. What does “Security Awareness Training” focus on?

A. Educating employees about security policies, practices, and the importance of security

B. Training IT staff on network configurations

C. Scheduling regular system updates and patches

D. Explaining legal responsibilities regarding data protection

*Security Awareness Training primarily aims to educate employees about security policies, practices, and the significance of maintaining security in an organizational context. This type of training is essential as it empowers employees to recognize potential security threats, understand their responsibilities in protecting sensitive information, and respond appropriately in various situations, such as encountering phishing attempts or handling confidential data. By focusing on the overall awareness of security measures, employees can become active participants in maintaining a secure environment, rather than passive observers. This proactive approach helps mitigate risks associated with human errors, which are often a significant factor in successful cyber attacks. While the other options mention important aspects of security, they address different areas of focus. For instance, training IT staff on network configurations is critical for technical security but does not encompass the broader employee base that security awareness training aims to reach. Regular system updates and patches fall under system maintenance and management, which is essential but separate from employee education. Finally, explaining legal responsibilities regarding data protection is vital for compliance purposes but does not encompass the holistic approach of security awareness that includes practical application and daily security practices employees must follow.*

## 7. What term describes a subject that is compliant and agreeable with a security personnel?

A. Cooperative

B. Compliant

C. Resistant

D. Nonchalant

*The term that best describes a subject that is compliant and agreeable with security personnel is "cooperative." This term signifies an individual who is willing to work with others, in this case, security personnel. When someone is cooperative, they actively participate in the process, follow instructions, and assist in achieving a safe and orderly environment. This behavior is crucial in security contexts where collaboration can enhance effectiveness and reduce misunderstandings or conflicts. "Compliant" could also describe someone who adheres to rules or directives, but it does not inherently convey an openness to collaboration or participation to the same extent as "cooperative." On the other hand, "resistant" denotes an unwillingness to comply or cooperate, and "nonchalant" indicates a lack of concern or indifference, which does not align with the notion of being agreeable or engaged with security personnel. Understanding these distinctions helps clarify why "cooperative" is the ideal choice for this scenario.*

## 8. What is the primary goal of the Situational Assessment process?

A. To find weaknesses in a team

B. To evaluate threats and dynamics

C. To generate reports on incidents

D. To train new personnel

*The primary goal of the Situational Assessment process is to evaluate threats and dynamics. This process involves analyzing the current environment to understand the various factors that could impact security, including potential risks, vulnerabilities, and the overall landscape that must be navigated. In this context, the assessment seeks to identify and evaluate specific threats that could compromise safety or security. It also examines the dynamics at play, such as relationships among different entities, changes in behavior, and external influences that could affect the security posture. This understanding enables organizations to make informed decisions, allocate resources effectively, and develop strategies to mitigate risks. Identifying threats and assessing their relevance and impact is crucial for establishing a proactive security posture rather than a reactive one. It's essential for shaping policies, enhancing preparedness, and ensuring that responses to incidents are adequate. While identifying weaknesses in a team, generating reports on incidents, or training new personnel can be important aspects of a security strategy, they do not encapsulate the primary focus of the Situational Assessment process, which is primarily directed at understanding the threats and contextual factors that need to be addressed.*

## 9. 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.*

**10. What does relative positioning refer to in the context of security personnel?**

A. The distance a subject maintains from the SP

B. The SP's location compared to the subject's

C. The emotional distance between the SP and the subject

D. The physical size of the SP relative to the subject

*Relative positioning in the context of security personnel refers to the security personnel's location compared to that of the subject. This concept is crucial in security operations, as it helps in assessing threat levels and maintaining appropriate distance for effective monitoring and response. Understanding the positioning allows security professionals to create a tactical advantage, whether by keeping the subject within a certain range for observation or ensuring their own safety. The distance between the security personnel and the subject can influence the dynamics of a situation, impacting how potential threats are managed. It also helps in establishing control during engagements, as proper positioning can deter adversarial actions and enable a readiness to respond if necessary. This method of positioning is strategic, differing from other options that discuss distance specifically, emotional context, or physical size, which do not encapsulate the broader tactical perspective of relative positioning.*

# 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!