Advanced Security Training (AST) Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

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

A. Cooperative

B. Compliant

C. Resistant

D. Nonchalant

2. What does the Cheek portion of the handcuff contain?

A. Only the key hole

B. The mechanics, key hole, and connection to the chain

C. Only the chain

D. None of the above

3. What is the renewal process for AST licenses?

A. Retaking the course

B. Simply applying for a renewal

C. Taking a short refresher course

D. Nothing, they renew automatically

4. What's the intended effect of effective Tactical Communication?

A. To intimidate the subject

B. To achieve compliance and cooperation

C. To establish dominance

D. To evaluate risk

5. What role does patch management play in cybersecurity?

A. It ensures a system remains outdated

B. It helps maintain application and system security

C. It focuses on user training

D. It monitors internet speeds

6. What is the term used to describe a risk posed by individuals within an organization who may misuse insider information?

A. External threat

B. Insider threat

C. Cyber threat

D. Public threat

7. What does regular security auditing primarily assess?

A. Employee efficiency

B. Physical office layout

C. Security measures and vulnerabilities

D. Software sales performance

8. 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

9. Position 2 is described as being located in which area relative to the subject?

A. Directly behind the subject

B. In front of the subject

C. At the side of the subject's body

D. At a 45° angle behind the subject

10. What characteristic defines a subject who is actively resistant?

A. The subject physically assaults the SP

B. The subject responds positively to commands

C. The subject verbally complies with the SP's directions

D. The subject actively resists control without physical assault

Answers

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

Explanations

1. 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.

2. What does the Cheek portion of the handcuff contain?

A. Only the key hole

B. The mechanics, key hole, and connection to the chain

C. Only the chain

D. None of the above

The Cheek portion of a handcuff is a crucial component that houses several important features. It contains the mechanics of the locking mechanism, which allows the handcuff to securely close around a wrist. This mechanism is vital for ensuring that the handcuff functions properly and cannot be easily tampered with or removed once applied. Additionally, the Cheek includes the keyhole, which is where the handcuff key is inserted to release the lock. This is an essential aspect of handcuff design, as it provides a means for authorized personnel to remove the restraint when necessary. Furthermore, the connection to the chain is also located in the Cheek portion, which is how the individual handcuffs are linked together. This design facilitates easy control and movement of a detained individual while ensuring that they remain properly secured. Overall, the Cheek of the handcuff effectively integrates these critical components—mechanics, keyhole, and connection to the chain—making it an integral part of the handcuff's functionality and security.

3. What is the renewal process for AST licenses?

A. Retaking the course

B. Simply applying for a renewal

C. Taking a short refresher course

D. Nothing, they renew automatically

The renewal process for AST licenses typically involves retaking the course. This approach ensures that license holders remain updated with the latest advancements and best practices in security training. Security protocols and technologies evolve rapidly, and by requiring individuals to retake the course, the licensing body ensures that practitioners have a current understanding of relevant concepts, laws, threats, and strategies. Continuing education is crucial in the field of security, as it helps professionals maintain competency in addressing new challenges and threats. The renewal process through course retaking emphasizes the importance of ongoing learning and skills enhancement within the industry, reflecting a commitment to professional growth and adherence to high standards of practice. In contrast, other options like simply applying for a renewal or taking a short refresher course might not provide the comprehensive knowledge necessary for effective license maintenance. Similarly, automatic renewals may lead to complacency and a lack of updated skills, which can be detrimental in a field where security landscapes continually change.

4. What's the intended effect of effective Tactical Communication?

A. To intimidate the subject

B. To achieve compliance and cooperation

C. To establish dominance

D. To evaluate risk

The intended effect of effective Tactical Communication is to achieve compliance and cooperation. This approach is essential in various situations, particularly in law enforcement and security contexts, where the goal is to manage interactions with individuals in a way that promotes safety and resolution. Effective communication techniques, which may include active listening, empathy, and clear instructions, help establish rapport and trust. This can lead to a more favorable outcome, such as de-escalation of a potentially volatile situation and the cooperation of the subject involved. Tactical communication focuses on understanding the needs and perspectives of others while guiding them towards a desired outcome without resorting to physical confrontation or coercion. By fostering compliance through positive engagement, security personnel can ensure both their safety and that of the individuals involved, ultimately allowing for a more peaceful resolution to conflicts.

5. What role does patch management play in cybersecurity?

A. It ensures a system remains outdated

B. It helps maintain application and system security

C. It focuses on user training

D. It monitors internet speeds

Patch management is a critical process in cybersecurity that involves the timely application of updates and patches to software and systems. This process helps to address vulnerabilities that could be exploited by attackers to gain unauthorized access or cause harm. By systematically managing patches, an organization can reduce its risk profile significantly, as many security breaches occur due to unpatched software that contains known vulnerabilities. When systems and applications are kept up to date through effective patch management, organizations can enhance their overall security posture. This includes fixing bugs, mitigating exploits, and ensuring compliance with regulatory standards. The ongoing maintenance of application and system security directly contributes to the prevention of data breaches and the protection of sensitive information from cyber threats. Therefore, the role of patch management is essential in safeguarding the integrity and availability of information systems in a proactive manner.

6. What is the term used to describe a risk posed by individuals within an organization who may misuse insider information?

A. External threat

B. Insider threat

C. Cyber threat

D. Public threat

The term "insider threat" specifically refers to risks that arise from individuals within the organization who have access to sensitive information and may misuse it for malicious purposes, whether intentionally or unintentionally. This can include employees, contractors, or business partners who exploit their access to data, systems, or resources, posing a significant security risk to the organization. Insider threats can manifest in various ways, such as data theft, sabotage, or the unintentional compromise of security protocols due to negligence. Being aware of insider threats is crucial for organizations so that they can implement proper security measures, such as access controls, monitoring, and employee training to mitigate these risks. In contrast, external threats originate from outside the organization and often involve hackers or cybercriminals attempting to compromise systems and steal data. Cyber threats encompass a range of malicious activities that exploit technological vulnerabilities, while public threats relate to risks that impact the organization as a whole but do not necessarily stem from within its ranks. Understanding the specific nature of insider threats enables organizations to develop targeted strategies for detection, prevention, and response.

7. What does regular security auditing primarily assess?

A. Employee efficiency

B. Physical office layout

C. Security measures and vulnerabilities

D. Software sales performance

Regular security auditing primarily assesses security measures and vulnerabilities within an organization. This process involves systematically reviewing and evaluating the effectiveness of security controls and procedures. Auditors look for weaknesses that could be exploited by malicious actors and assess the overall security posture of the organization. Through security audits, organizations can identify gaps in their defenses, ensure compliance with relevant regulations and standards, and improve their incident response strategies. The focus is on protecting sensitive data, maintaining system integrity, and addressing potential risks that may arise from both internal and external threats. While the other options touch on various aspects of an organization's function, they do not pertain to the specific goals and objectives of security auditing. Employee efficiency relates to productivity and human resources, physical office layout refers to the design and use of physical space, and software sales performance focuses on business sales metrics, none of which address the core objectives of identifying and mitigating security risks.

8. 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.

9. Position 2 is described as being located in which area relative to the subject?

A. Directly behind the subject

B. In front of the subject

C. At the side of the subject's body

D. At a 45° angle behind the subject

The choice that identifies Position 2 as being at the side of the subject's body is the most accurate because it suggests a relative positioning that is often used in various security scenarios. This position can provide a strong vantage point for monitoring the subject without being directly in their line of sight, which may help in assessing situations discreetly or maintaining an appropriate level of engagement with the subject. Positioning at the side can also facilitate communication and movement. For example, in a security context, being at the side allows for greater awareness of the environment while still being close enough to intervene if necessary. This is particularly important in situations where situational awareness is critical and observing a subject's behavior is part of the security protocol.

10. What characteristic defines a subject who is actively resistant?

A. The subject physically assaults the SP

B. The subject responds positively to commands

C. The subject verbally complies with the SP's directions

D. The subject actively resists control without physical assault

A subject who is actively resistant is characterized by their refusal to comply with the control efforts of a security personnel (SP) despite not engaging in physical assault. This means the individual may show defiance through behaviors such as resisting verbal commands, failing to follow instructions, or attempting to evade control. In this context, actively resisting control can manifest through physical movements that are intended to break free or avoid being apprehended, as well as non-verbal cues that indicate refusal to cooperate. This type of resistance is crucial for security personnel to recognize, as it determines how they should respond, including the application of appropriate de-escalation techniques. The other choices illustrate different behaviors that do not fit the definition of active resistance. Physical assault involves an escalation of violence, while positive responses to commands and verbal compliance indicate cooperation rather than resistance. Understanding the distinction of active resistance is essential in security training and management strategies.