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

## Study Guide

BY EXAMZIFY

**Everything you need from our exam experts!**

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

# Questions

**1. What does the principle of least privilege entail?**

**A. Users have unrestricted access to all resources**

**B. Users' access rights are limited to the bare minimum needed**

**C. Data is accessible to all employees for transparency**

**D. Privileged accounts require multiple verifications for access**

**2. What is the primary function of encryption?**

**A. To validate user identities**

**B. To ensure data availability**

**C. To protect the confidentiality of data**

**D. To monitor network traffic**

**3. What is the main role of an Intrusion Detection System (IDS)?**

**A. To enhance network speed and efficiency**

**B. To monitor network traffic for suspicious activity**

**C. To automatically block unauthorized access**

**D. To create backups of critical data**

**4. 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**

**5. What does the CIA triad stand for in information security?**

**A. Confidentiality, Integrity, and Availability**

**B. Control, Impact, and Assurance**

**C. Classification, Identification, and Authentication**

**D. Compliance, Integrity, and Accountability**

**6. What is the purpose of a vulnerability assessment?**

**A. To improve employee knowledge of security risks**

**B. To evaluate the effectiveness of firewalls**

**C. To identify weaknesses that may be exploited**

**D. To enhance physical infrastructure**

**7. 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**

**8. What does two-factor authentication (2FA) entail?**

**A. Verifying identity through a single piece of information**

**B. Requiring users to verify their identity using two different forms of authentication**

**C. Using biometric authentication methods only**

**D. Implementing password complexity requirements**

**9. What defines a security incident?**

**A. A minor breach of data that does not affect systems**

**B. An event that compromises the integrity, confidentiality, or availability of information**

**C. Any unauthorized access attempt to the network**

**D. A predicted assessment of potential threats**

**10. What is a security token used for?**

**A. A physical device for storing passwords**

**B. A method to encrypt data**

**C. A device to authenticate a user’s identity**

**D. A tool for monitoring network traffic**

# Answers

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

# Explanations

## 1. What does the principle of least privilege entail?

A. Users have unrestricted access to all resources

B. Users' access rights are limited to the bare minimum needed

C. Data is accessible to all employees for transparency

D. Privileged accounts require multiple verifications for access

**The principle of least privilege is a fundamental concept in security that states that users should be granted the minimum levels of access necessary to perform their job functions. This principle aims to limit potential damage in the event of a security breach, reduce the attack surface for malicious actors, and prevent unauthorized access to sensitive information.  By ensuring that users have only the bare minimum permissions required for their roles, organizations can enhance their security posture. This minimizes the risk of accidental or intentional misuse of information and resources, safeguarding against data breaches and maintaining the confidentiality, integrity, and availability of systems. The other options do not align with the principle of least privilege: unrestricted access to resources would create significant security risks; data accessibility for all employees can lead to information exposure and breaches; and requiring multiple verifications for privileged accounts, while important, is a separate security measure related to authentication rather than a direct application of the least privilege principle.**

## 2. What is the primary function of encryption?

A. To validate user identities

B. To ensure data availability

C. To protect the confidentiality of data

D. To monitor network traffic

**Encryption is primarily utilized to protect the confidentiality of data. This involves converting readable information (plaintext) into an encoded format (ciphertext) that can only be read or decrypted by someone with the appropriate key or password. The main purpose of encryption is to shield sensitive information from unauthorized access, ensuring that even if the data is intercepted or accessed by an adversary, it remains unintelligible without the necessary decryption mechanism.  This fundamental aspect of data confidentiality is critical in various domains, such as securing personal information, financial data, and communications, thereby maintaining privacy and safeguarding against data breaches. By implementing encryption, organizations can effectively mitigate the risk associated with data exposure, which can lead to severe consequences ranging from financial loss to compromised personal data.**

## 3. What is the main role of an Intrusion Detection System (IDS)?

A. To enhance network speed and efficiency

B. To monitor network traffic for suspicious activity

C. To automatically block unauthorized access

D. To create backups of critical data

**The primary role of an Intrusion Detection System (IDS) is to monitor network traffic for suspicious activity. An IDS analyzes incoming and outgoing data packets within a network to detect patterns that may indicate malicious behavior or security breaches. By identifying anomalies or known threat signatures, the IDS can alert network administrators to potential attacks, enabling them to take appropriate action to mitigate risks. This active monitoring allows organizations to gain visibility into their security posture, respond to threats in real-time, and maintain the integrity of their systems. While enhancing network speed, blocking unauthorized access, and creating backups are crucial tasks for a comprehensive security program, they fall under the functions of other security systems or practices rather than the specific role of an IDS. An IDS focuses solely on detection, allowing it to specialize in identifying and reporting potential threats rather than executing defensive actions.**

## 4. 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.**

## 5. What does the CIA triad stand for in information security?

A. Confidentiality, Integrity, and Availability

B. Control, Impact, and Assurance

C. Classification, Identification, and Authentication

D. Compliance, Integrity, and Accountability

**The CIA triad is a foundational concept in information security that stands for Confidentiality, Integrity, and Availability. Each component represents a key principle that organizations must address to protect their information systems and data. Confidentiality ensures that sensitive information is accessed only by authorized individuals. This is critical in preventing unauthorized access and safeguarding personal data, trade secrets, and proprietary information. Integrity pertains to maintaining the accuracy and completeness of data over its entire lifecycle. This means ensuring that data remains unaltered except by authorized users and is accurately reflected in information systems. Protecting data integrity is crucial to ensure that information is trustworthy and can be relied upon for decision-making. Availability refers to ensuring that information and resources are accessible to authorized users when needed. This involves implementing measures to mitigate downtime and ensuring systems remain operational, even during attacks or failures. Together, these three principles form the basis for a comprehensive security strategy, as neglecting any one of them can compromise the overall security posture of an organization. Understanding the CIA triad is essential for anyone involved in the field of information security, as it influences design decisions, risk management, and policy creation.**

## 6. What is the purpose of a vulnerability assessment?

A. To improve employee knowledge of security risks

B. To evaluate the effectiveness of firewalls

C. To identify weaknesses that may be exploited

D. To enhance physical infrastructure

**The purpose of a vulnerability assessment is to identify weaknesses that may be exploited in an organization's systems, applications, or networks. This process involves a systematic review of the security measures in place, as well as the potential areas of vulnerability, which could be exploited by malicious actors. By identifying these vulnerabilities, organizations can prioritize the risks and implement appropriate measures to mitigate them, thus enhancing their overall security posture. In the context of cybersecurity, this assessment plays a critical role in understanding the threat landscape and helps organizations take proactive steps to safeguard their assets against potential security breaches. The focus is squarely on detecting shortcomings that could lead to unauthorized access, data breaches, or other security incidents. While improving employee knowledge of security risks, evaluating the effectiveness of firewalls, and enhancing physical infrastructure are all important elements of a comprehensive security strategy, they do not directly encapsulate the primary goal of a vulnerability assessment, which remains focused on identifying specific vulnerabilities that could be exploited.**

### 7. 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.**

### 8. What does two-factor authentication (2FA) entail?

A. Verifying identity through a single piece of information

B. Requiring users to verify their identity using two different forms of authentication

C. Using biometric authentication methods only

D. Implementing password complexity requirements

**Two-factor authentication (2FA) is a security mechanism designed to enhance the protection of user accounts by requiring the use of two different forms of authentication. This method typically combines something the user knows (like a password) with something the user has (such as a smartphone for a text message or an authentication application) or something the user is (like a fingerprint or facial recognition). The key component of 2FA is the dual-layered approach, which significantly reduces the likelihood of unauthorized access because an attacker would need to obtain both pieces of information to successfully gain entry to an account.  In contrast, verifying identity through a single piece of information does not meet the requirements of 2FA, as it lacks the second factor necessary for enhanced security. Relying exclusively on biometric methods narrows the focus to just one type of authentication, which does not constitute two-factor authentication unless combined with another method. Additionally, implementing password complexity requirements, while important for securing passwords, does not involve the use of a second authentication factor and therefore does not classify as 2FA.**

## 9. What defines a security incident?

A. A minor breach of data that does not affect systems

B. An event that compromises the integrity, confidentiality, or availability of information

C. Any unauthorized access attempt to the network

D. A predicted assessment of potential threats

A security incident is defined as an event that compromises the integrity, confidentiality, or availability of information. This definition encompasses a wide scope of potential issues that can arise within an organization and highlights the fundamental aspects of information security. When we talk about integrity, we're addressing the accuracy and trustworthiness of data; confidentiality refers to the measures in place to protect information from unauthorized access; and availability ensures that data and systems are accessible when needed. A situation that affects even one of these pillars can be deemed a security incident, as it poses a risk to the overall security posture of the organization. The other options do not capture the completeness of what constitutes a security incident. While a minor breach of data or unauthorized access attempts are concerning, they do not necessarily involve a significant compromise of the broader aspects of information security. Predicting potential threats is part of risk management rather than direct implications of an actual incident. Therefore, understanding a security incident requires a holistic approach that aligns with the definition of compromising the key principles of information security.

## 10. What is a security token used for?

A. A physical device for storing passwords

B. A method to encrypt data

C. A device to authenticate a user’s identity

D. A tool for monitoring network traffic

A security token is primarily used as a device to authenticate a user’s identity. Its main function is to generate a unique one-time password or security code that verifies a user's credentials during the authentication process. This ensures that the individual trying to access a system is indeed authorized to do so, enhancing security by providing an additional layer beyond just a username and password. Security tokens can come in various forms, such as hardware tokens (physical devices that generate codes) or software tokens (applications that provide similar functionality). By requiring something the user has (the token) along with something they know (their password), security tokens significantly reduce the risk of unauthorized access, making them a vital component in multi-factor authentication strategies. The other options describe different security mechanisms that do not directly relate to the primary function of a security token. For instance, while a physical device for storing passwords serves as a secure storage solution, it does not actively authenticate users. Encryption methods protect data integrity and confidentiality but are not used directly for user authentication. Monitoring network traffic, on the other hand, involves analyzing data flow within a network and is unrelated to the processes associated with user authentication.