# SANS Security's Foundation Practice Test (Sample)

## Study Guide

BY EXAMZIFY

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

**Sample study guide. Visit https://sanssecurityfoundation.examzify.com**

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

# Questions

**1. What does risk acceptance imply in a business context?**

**A. Eliminating all potential risks faced**

**B. Allowing certain risks to exist after mitigation strategies**

**C. Implementing extensive control measures**

**D. Documenting every possible risk scenario**

**2. What technique is used to ensure data integrity in transit?**

**A. Encryption**

**B. Hashing**

**C. Tokenization**

**D. Decryption**

**3. What is endpoint security?**

**A. Monitoring network traffic**

**B. Protecting devices that connect to a network**

**C. Managing user access to systems**

**D. Analyzing security logs**

**4. Which of the following activities is associated with the response phase of incident management?**

**A. Conducting audits**

**B. Implementing authentication measures**

**C. Planning for disaster recovery**

**D. Executing an incident response plan**

**5. What does maximum password aging refer to?**

**A. Changing password at any time**

**B. When you must change your password after a period of time**

**C. Not needing to change your password**

**D. Not having any aging policy**

**6. Why is tracking activity important in accountability?**

**A. It allows employees to avoid their responsibilities**

**B. It helps in assessing performance and development**

**C. It reduces the workload for managers**

**D. It distracts from core functions of work**

7. **Which item is considered a part of physical security measures?**

   A. **Incident response plans**

   B. **Cameras**

   C. **Anti-virus software**

   D. **Data encryption tools**

8. **What does a threat model assess?**

   A. **Potential software updates**

   B. **Browser vulnerabilities**

   C. **Potential threats and vulnerabilities**

   D. **User training effectiveness**

9. **What does "something you have" authentication typically refer to?**

   A. **A fingerprint**

   B. **A token you hold in your hand**

   C. **A password you memorize**

   D. **A voice print**

10. **Which component of AAA focuses on validating user privileges?**

   A. **Authentication**

   B. **Authorization**

   C. **Accountability**

   D. **Access Control**

# Answers

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

# Explanations

## 1. What does risk acceptance imply in a business context?

- A. Eliminating all potential risks faced
- B. Allowing certain risks to exist after mitigation strategies
- C. Implementing extensive control measures
- D. Documenting every possible risk scenario

**Risk acceptance in a business context signifies that an organization acknowledges the presence of certain risks and decides to allow them to persist after having implemented suitable mitigation strategies. This approach implies a calculated decision where the potential impact and likelihood of the risks are weighed against the costs and feasibility of further mitigation efforts. Accepting risk does not mean ignoring it; rather, it involves a thorough assessment of risks and a thoughtful decision-making process regarding which risks to manage actively and which can be tolerated. The rationale behind this strategy can vary – it might be due to the costs of additional control measures being higher than the potential impact of the risk, or perhaps the organization believes that existing controls adequately minimize the threat. In contrast, eliminating all potential risks is often impractical or unrealistic, as risk is inherent to any business operation. Implementing extensive control measures can lead to over-engineering, where the costs outweigh the benefits. Documenting every possible risk scenario can also become unmanageable and detracts from focusing on those risks that are most critical to the organization’s objectives and operational integrity. Thus, risk acceptance is a strategic approach that recognizes the balance between risk and reward in the context of business operations.**

## 2. What technique is used to ensure data integrity in transit?

- A. Encryption
- B. Hashing
- C. Tokenization
- D. Decryption

**Hashing is a technique used to ensure data integrity in transit by creating a fixed-size string of characters from input data, regardless of its size. This string, often referred to as a hash value or checksum, is generated through a specific algorithm that produces a unique value for different sets of input data. When data is sent over a network, the sender can compute the hash of the original data and send both the data and the hash value to the receiver. Upon receipt, the receiver will compute the hash of the received data and compare it to the hash value sent by the sender. If both hash values match, it indicates that the data has not been altered during transit, thereby ensuring its integrity. This process does not obscure the data but confirms its authenticity and completeness. Other techniques serve different purposes; for example, encryption primarily protects confidentiality by transforming data into an unreadable format for unauthorized users, while tokenization replaces sensitive data with non-sensitive equivalents to minimize exposure to risk. Decryption is the reverse of encryption, aiming to restore the readable form of encrypted data, but it does not verify data integrity.**

## 3. What is endpoint security?

A. Monitoring network traffic

B. Protecting devices that connect to a network

C. Managing user access to systems

D. Analyzing security logs

**Endpoint security refers to the strategy and tools aimed at protecting devices that connect to a network, such as computers, smartphones, tablets, and servers. The primary focus of endpoint security is to safeguard these devices from threats like malware, unauthorized access, and other security vulnerabilities. By implementing endpoint security, organizations can ensure that each point of entry into their network is secured, thereby reducing the risk of data breaches and cyberattacks. This is critical as each endpoint can serve as a potential attack vector for cybercriminals seeking to exploit vulnerabilities within the network. Other options address important aspects of security but do not encapsulate the specific focus of endpoint security. Monitoring network traffic is a broader practice involving observation of data packets traversing the network, while managing user access is essential for controlling who can access specific systems or data. Analyzing security logs is crucial for identifying suspicious activities and maintaining security but is not confined to the specific protection of endpoint devices.**

## 4. Which of the following activities is associated with the response phase of incident management?

A. Conducting audits

B. Implementing authentication measures

C. Planning for disaster recovery

D. Executing an incident response plan

**The response phase of incident management focuses on actions taken after a security incident has been detected. This phase involves executing predetermined processes to handle the incident, mitigate its impact, recover from it, and prevent future occurrences. Specifically, executing an incident response plan is central to this phase, as it outlines the necessary steps and measures that should be implemented when an incident occurs, including identification, containment, eradication, and recovery. The other activities, such as conducting audits, implementing authentication measures, and planning for disaster recovery, are critical components of overall security and risk management but do not fall under the immediate actions taken during the incident response phase. Conducting audits might help identify vulnerabilities, implementing authentication measures enhances security posture, and planning for disaster recovery is essential for maintaining business continuity, but these actions are typically part of preparedness and preventive strategies rather than direct responses to active incidents.**

## 5. What does maximum password aging refer to?

A. Changing password at any time

B. When you must change your password after a period of time

C. Not needing to change your password

D. Not having any aging policy

Maximum password aging refers to a security practice where users are required to change their passwords after a predetermined period of time. This is implemented to enhance security by reducing the risk of unauthorized access that could occur if credentials are compromised but not updated. By establishing a time limit for password validity, organizations can minimize the potential for long-term exploitation of stagnant credentials. The practice of setting a maximum password age helps ensure that even if a password is discovered or stolen, its utility for an attacker is limited due to the requirement to change it regularly. This mechanism encourages users to actively maintain their account security and stay vigilant about their authentication practices.

## 6. Why is tracking activity important in accountability?

A. It allows employees to avoid their responsibilities

B. It helps in assessing performance and development

C. It reduces the workload for managers

D. It distracts from core functions of work

Tracking activity is essential for accountability because it provides a measurable framework for assessing performance and development. By monitoring what tasks individuals and teams engage in, organizations can evaluate how effectively employees carry out their responsibilities, identify strengths and weaknesses, and recognize areas where further development is needed. This process not only aids in performance reviews but also facilitates targeted training and growth opportunities, fostering an environment where employees can improve and succeed. Beyond performance assessment, tracking can lead to increased transparency, allowing both employees and managers to understand expectations and outcomes better. This accountability helps in aligning individual contributions with organizational goals, thereby enhancing overall productivity. The other options do not align with the principles of accountability. For instance, avoiding responsibilities or reducing managerial workload runs counter to promoting accountability, while distractions detract from the focus necessary for achieving work goals. Thus, the primary value of tracking activity lies unequivocally in enhancing performance assessment and professional development.

## 7. Which item is considered a part of physical security measures?

**A. Incident response plans**

**B. Cameras**

**C. Anti-virus software**

**D. Data encryption tools**

**Cameras are a key component of physical security measures because they are used to monitor and record activities in and around a facility. Their primary purpose is to deter unauthorized access, identify intruders, and provide security personnel with real-time data that can be used for incident investigations. In contrast, incident response plans, anti-virus software, and data encryption tools fall under different categories of security. Incident response plans are focused on handling security incidents, anti-virus software deals with protecting information systems from malware, and data encryption tools are used to secure data at rest and in transit. Therefore, the integration and functionality of cameras as a surveillance tool clearly position them within the realm of physical security measures, making them the correct choice in this context.**

## 8. What does a threat model assess?

**A. Potential software updates**

**B. Browser vulnerabilities**

**C. Potential threats and vulnerabilities**

**D. User training effectiveness**

**A threat model is primarily focused on identifying and evaluating potential threats and vulnerabilities that an organization may face. This process involves analyzing the assets that need protection, understanding the potential adversaries and their capabilities, and determining the ways these adversaries could exploit vulnerabilities in a system. By establishing a clear picture of threats, organizations can prioritize their security efforts, design defensive measures, and enhance their overall security posture. In contrast, assessing potential software updates focuses on evaluating new software changes for risks, browser vulnerabilities specifically target weaknesses in web browsers, and user training effectiveness evaluates how well users understand and adhere to security protocols. While each of these areas is important for a comprehensive security strategy, they do not capture the broader assessment that a threat model provides.**

## 9. What does "something you have" authentication typically refer to?

A. A fingerprint

B. A token you hold in your hand

C. A password you memorize

D. A voice print

"Something you have" authentication refers to a method of verifying a user's identity based on a physical object or token that they possess. In this context, a token you hold in your hand is a classic example of this type of authentication. This could be a hardware token, smart card, or mobile device that generates a unique code. It acts as an additional layer of security because even if someone's password were compromised, they would also need physical access to the token to gain entry. The other options provided do not fit the definition of "something you have." A fingerprint and a voice print are examples of "something you are" authentication, as they rely on unique biological traits for verification. A password you memorize falls under "something you know" authentication, which is distinct from token-based approaches. These distinctions highlight the importance of "something you have" as a tangible element in the authentication process.

## 10. Which component of AAA focuses on validating user privileges?

A. Authentication

B. Authorization

C. Accountability

D. Access Control

The component of AAA that focuses on validating user privileges is authorization. This process involves determining what resources a user is allowed to access and what actions they can perform once authenticated. After a user has successfully proven their identity through authentication, authorization comes into play to ensure that they only have access to the resources and actions that align with their assigned permissions or roles. When a user attempts to access a resource, the system checks their credentials against pre-defined access control policies to ascertain their level of access. This ensures security by preventing users from engaging in actions or accessing information beyond their permissions, thereby minimizing the risk of unauthorized data access or manipulation. In the context of security frameworks, it's essential to establish distinct boundaries between authentication (verifying identity), authorization (determining access rights), accountability (tracking actions taken by users), and access control (the mechanisms that enforce permissions). Understanding these distinctions is critical for effectively managing user access and maintaining system integrity.