INFORMATION SECURITY PRINCIPLES AND FRAMEWORKS PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://infosecprinciplesframeworks.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 type of security control acts during an incident to identify or record that the incident is happening?**

   A. Deterrent

   B. Detective

   C. Directive

   D. Compensating

2. **A group account is a collection of user accounts used to grant the same level of access to multiple users. What is this concept called?**

   A. Permissions

   B. Group Account

   C. Discretionary Access Control (DAC)

   D. RBAC

3. **What process determines what rights and privileges an entity has?**

   A. Authentication

   B. Identification

   C. Accounting

   D. Authorization

4. **Which port is commonly used by the Remote Desktop Protocol?**

   A. 3389

   B. 22

   C. 80

   D. 443

5. **Which term denotes a token that represents the ownership factor in a multifactor authentication scheme, generated by a hardware device?**

   A. Hard authentication token

   B. Security key

   C. Smart cards

   D. Biometric authentication

6. Which term refers to a short-range wireless radio transmission medium used to connect two personal devices, such as a mobile phone and a wireless headset?

A. Bluetooth

B. NFC

C. TLS

D. GPS

7. Which term describes detective and preventive security controls that use an agent or network configuration to monitor hosts, allowing for more accurate credentialed scanning, but consumes some host resources and is detectable by threat actors?

A. Network-based control

B. Credentialed scanning

C. Host-based control

D. Active security control

8. A cloud service model that provisions application and database services as a platform for development of apps.

A. Software as a Service (SaaS)

B. Cloud service models

C. Anything as a Service (XaaS)

D. Platform as a Service (PaaS)

9. In EAP architecture, which entity is the device requesting access to the network?

A. Authenticator

B. RADIUS

C. Supplicant

D. Compute

10. What term describes serverless computing offloading infrastructure management to the cloud provider, such as configuring storage without building and deploying a file server?

A. Serverless computing

B. Virtual machines

C. Container orchestration

D. On-premises hosting

Answers

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

Explanations

1. Which type of security control acts during an incident to identify or record that the incident is happening?

A. Deterrent

B. Detective

C. Directive

D. Compensating

Detective security controls identify and record events as they occur. They monitor the environment and generate alerts or logs when something suspicious happens, so an incident can be detected in real time and evidence can be collected. Examples include intrusion detection systems, security information and event management (SIEM), access logs, and continuous monitoring. Deterrent controls aim to discourage attacks before they happen and do not provide real-time identification. Directive controls are policies and procedures that guide how people should behave, rather than actively detecting incidents. Compensating controls provide an alternative safeguard when the primary control isn't feasible, but they're not defined primarily by their ability to detect incidents.

2. A group account is a collection of user accounts used to grant the same level of access to multiple users. What is this concept called?

A. Permissions

B. Group Account

C. Discretionary Access Control (DAC)

D. RBAC

The idea being tested is using a shared container to grant the same access to many people. A group account acts as a single identity that represents a set of user accounts; when permissions are given to that group account, every member of the group inherits those rights. This makes administration simpler because you manage access at the group level rather than configuring permissions for each individual user, and you can add or remove members to adjust who has the access. Other terms point to different ideas: permissions are the actual rights granted, not the container that holds multiple users; discretionary access control is a model where owners decide who can access resources; and RBAC is a system that assigns permissions to roles which are then assigned to users. The concept described—a single account representing multiple users to provide the same access—is best described as a group account.

3. What process determines what rights and privileges an entity has?

A. Authentication

B. Identification

C. Accounting

D. Authorization

Authorization determines what rights and privileges an entity has. It happens after authentication, when the system applies policies to decide what a user or process is allowed to do with resources. In practice, once identity is verified, the system checks roles, attributes, or rules (such as ACLs or RBAC) to grant or deny specific actions like read, write, or execute. This separation matters: authentication verifies who you are, identification is the claimed identity, and accounting logs what you did. For example, after logging in (authentication), a user's role is consulted to determine if they can access a file or perform a change (authorization).

4. Which port is commonly used by the Remote Desktop Protocol?

A. 3389

B. 22

C. 80

D. 443

Remote Desktop Protocol relies on a dedicated TCP port by default, which is the one most commonly associated with and expected for RDP connections. That default port is what makes it the best answer here, because knowing this port helps you configure firewalls and access controls around RDP. The other ports correspond to different services you might see on a network—SSH for secure remote login, HTTP for web traffic, and HTTPS for secure web traffic—so they're not the standard port used by RDP. While you can reconfigure RDP to listen on another port, using the default port is the common, recognized choice, and it's important to secure it properly (for example, by restricting exposure to the internet and using VPN or a gateway).

5. Which term denotes a token that represents the ownership factor in a multifactor authentication scheme, generated by a hardware device?

A. Hard authentication token

B. Security key

C. Smart cards

D. Biometric authentication

Ownership as a factor in multifactor authentication means you must prove you possess something physical. A hardware device that generates a code or cryptographic response on demand is a hard authentication token—the classic physical token used to demonstrate you have the device. This token is produced by the device itself and changes over time or per event, which is exactly what shows possession of the hardware. Biometric authentication isn't an ownership factor but a "something you are" factor. Smart cards are hardware credentials and can serve as possession devices, but the term that emphasizes the generated token from the hardware device is hard authentication token. A security key is a hardware credential as well, but the phrasing here centers on the token generated by the device, which aligns with the hard token concept.

6. Which term refers to a short-range wireless radio transmission medium used to connect two personal devices, such as a mobile phone and a wireless headset?

A. Bluetooth

B. NFC

C. TLS

D. GPS

Bluetooth is the short-range wireless technology designed to connect personal devices like a smartphone and a wireless headset. It operates over the 2.4 GHz band and is optimized for low power, low data-rate links, which suits audio streaming and hands-free calling within about 10 meters. The key idea is creating a personal area network that can pair devices quickly and maintain a stable link for everyday use. NFC also handles short-range communication but only at very close proximity and mainly to initiate pairing or small data transfers, not for ongoing audio streams. TLS is a security protocol for protecting data over networks, not a radio transmission medium, and GPS is a satellite-based positioning system, not a device-to-device link. Bluetooth best fits the description of a short-range wireless medium connecting two personal devices.

7. Which term describes detective and preventive security controls that use an agent or network configuration to monitor hosts, allowing for more accurate credentialed scanning, but consumes some host resources and is detectable by threat actors?

A. Network-based control

B. Credentialed scanning

C. Host-based control

D. Active security control

Host-based controls involve security measures that reside on endpoints or rely on endpoint configurations to monitor the system. By using an agent installed on each host or a specific network configuration targeting the host, these controls can perform credentialed scanning—checking the system from within with valid credentials to assess things like patches, configurations, and policies with greater accuracy. Since the code and processes run on the host, they consume some CPU, memory, and I/O resources, and the presence of the agent or its activity can be detected by threat actors who monitor for unusual processes or services. This approach contrasts with network-based controls, which monitor traffic and do not require an agent on each host, and with credentialed scanning as a technique, which is about how you assess posture rather than the control's placement. An "active security control" is a broad label for mechanisms that actively monitor or enforce policies, but the described setup specifically points to host-based controls due to the agent on the host and the credentialed access it enables.

8. A cloud service model that provisions application and database services as a platform for development of apps.

A. Software as a Service (SaaS)

B. Cloud service models

C. Anything as a Service (XaaS)

D. Platform as a Service (PaaS)

Platform as a Service provides a ready-to-use environment for building and deploying applications, including the runtime, development tools, and database services that developers need. The description—provisions application and database services as a platform for development of apps—fits this model because it emphasizes a development platform rather than delivering finished software or just raw infrastructure. SaaS would give you end-user software to use, not a development platform. XaaS is a broad umbrella term for anything-as-a-service. IaaS offers underlying compute, storage, and networking resources, not a full development platform with integrated app services.

9. In EAP architecture, which entity is the device requesting access to the network?

A. Authenticator

B. RADIUS

C. Supplicant

D. Compute

In EAP architecture, the device that wants to connect to the network is the supplicant. In this model, three roles exist: the supplicant (the client device requesting access), the authenticator (the network device such as a switch or wireless access point that enforces access control and passes authentication messages), and the authentication server (often a RADIUS server) that validates credentials. The supplicant initiates the authentication process, sending its credentials through the authenticator to the authentication server. The authenticator doesn't make the access decision by itself; it simply gates the port based on the server's response. The term compute isn't a defined role in this context. So the device requesting access is the supplicant.

10. What term describes serverless computing offloading infrastructure management to the cloud provider, such as configuring storage without building and deploying a file server?

A. Serverless computing

B. Virtual machines

C. Container orchestration

D. On-premises hosting

Serverless computing offloads the responsibility for provisioning, patching, scaling, and maintaining the underlying servers to the cloud provider. You focus on what you want to run or configure—like storage—without building and deploying a dedicated file server yourself. The provider handles the infrastructure, and you typically pay only for what you use, with automatic scaling. This fits because it describes configuring storage in a managed way without setting up and operating your own server infrastructure. In contrast, virtual machines require you to manage the operating system and server details, container orchestration still involves managing a cluster of containers, and on-premises hosting means running everything in your own data center rather than in the cloud.

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://infosecprinciplesframeworks.examzify.com

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