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

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

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

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 15

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. **Which authentication technology enables a user to authenticate once and receive authorizations for multiple services?**

   A. Multifactor Authentication (MFA)

   B. Single Sign-On (SSO)

   C. OAuth 2.0

   D. OpenID Connect

2. **Which statement best describes the SHA family?**

   A. Hashing

   B. Encryption

   C. Public Key

   D. Symmetric

3. **Which Windows feature centralizes the configuration and deployment of user and computer settings across a domain?**

   A. Active Directory Domain Services

   B. Group Policy Objects (GPOs)

   C. DNS Policy

   D. Local Users and Groups

4. **Which security control configuration blocks access to a resource in the event of a failure?**

   A. Fail-closed

   B. Fail-open

   C. Router firewall

   D. State table

5. **The likelihood and impact (consequence) of a threat actor exercising a vulnerability is called?**

   A. Risk

   B. Threat

   C. Impact

   D. Exposure

SAMPLE

6. Which term refers to a security solution designed to manage and control cloud service usage across users and devices?

A. Credentialed scan

B. Vulnerability scanner

C. Cloud identity and access management

D. Cloud access security broker (CASB)

7. Which term refers to hardware or software used on a private network without the owner's knowledge?

A. Shadow IT

B. Unauthorized

C. Hacker

D. Internal threat

8. What security control enforces a virtual boundary based on real-world geography?

A. Geofencing

B. Geolocation-based access control

C. Geo-blocking

D. Geographic boundary enforcement

9. Which term describes a guided, non-live exercise used to discuss response to events?

A. Drill

B. Live Exercise

C. Functional Test

D. Tabletop Exercises

10. Which architectural style is described as stateless and uses standard operations for web services?

A. GraphQL

B. SOAP

C. REST

D. RPC

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which authentication technology enables a user to authenticate once and receive authorizations for multiple services?

A. Multifactor Authentication (MFA)

B. Single Sign-On (SSO)

C. OAuth 2.0

D. OpenID Connect

Single Sign-On lets you authenticate once with a central identity provider and then access multiple services without re-authenticating. After you log in, a session or token from the identity provider is trusted by each connected service, so you're authorized to use them without signing in again. That direct one-login-for-many-services behavior is exactly what SSO provides, making it the best fit for this scenario. Multifactor Authentication adds extra verification steps for a single login, but it doesn't by itself enable access to multiple services after one sign-in. OAuth 2.0 provides tokens to authorize apps to access resources, not a universal sign-on experience. OpenID Connect adds authentication on top of OAuth 2.0 and can enable SSO in many implementations, but the core capability described here—one login for multiple services—is the hallmark of Single Sign-On.

2. Which statement best describes the SHA family?

A. Hashing

B. Encryption

C. Public Key

D. Symmetric

SHA family are cryptographic hash functions that take input data and produce a fixed-length digest. They are designed to be deterministic, fast to compute, and one-way, with properties like preimage resistance and collision resistance, so you can't easily recover the original data or find two inputs that produce the same hash. This makes them ideal for verifying data integrity, supporting digital signatures, and hashing passwords (often with a salt). It isn't encryption, because there's no key to encrypt or decrypt, and hashes aren't reversible. It also isn't a public-key or symmetric algorithm, which rely on keys to transform data. Variants like SHA-256, SHA-512, and SHA-3 all serve the hashing purpose.

SAMPLE

3. Which Windows feature centralizes the configuration and deployment of user and computer settings across a domain?

A. Active Directory Domain Services

B. Group Policy Objects (GPOs)

C. DNS Policy

D. Local Users and Groups

Group Policy Objects are the mechanism that centralizes the configuration and deployment of user and computer settings across a domain. By creating policies in GPOs and linking them to tiers in Active Directory (sites, domains, or organizational units), administrators can enforce security settings, deploy software, map drives, configure desktop environments, and set user rights for many domain-joined machines and users from one place. Settings flow down the AD hierarchy and apply during startup or logon, with a clear precedence model so you can tailor what applies where. This enables consistent, scalable configuration management, rapid enforcement of baselines, and simpler compliance across the entire domain. Active Directory Domain Services is the directory service that stores and authenticates objects in the domain; it enables GPOs to exist and be applied, but the central mechanism for configuring and deploying those settings is the Group Policy feature itself. DNS Policy handles DNS-related decision-making and is not about configuring users and computers across a domain. Local Users and Groups manages accounts on individual machines and does not provide domain-wide policy deployment.

4. Which security control configuration blocks access to a resource in the event of a failure?

A. Fail-closed

B. Fail-open

C. Router firewall

D. State table

Fail-closed means that when the security control experiences a fault, it blocks access by default. This behavior protects the resource even if the control goes down or malfunctions, because the safest default is to deny entry rather than risk an open door. In practice, if a firewall or access-control device fails, a fail-closed configuration will drop traffic, keeping the resource secure. In contrast, fail-open would permit access when the control fails, increasing risk. The other options don't describe this failure-mode behavior: a router firewall is a device type, not a failure reaction; a state table is a mechanism for tracking connections, not a failure-state policy.

5. The likelihood and impact (consequence) of a threat actor exercising a vulnerability is called?

A. Risk

B. Threat

C. Impact

D. Exposure

In information security, risk is defined as the combination of how likely it is that a threat actor will exploit a vulnerability and the potential consequences if that exploitation occurs. This question points to that exact idea—risk merges both the probability of an event and the impact it would have. A threat is simply the actor or event that could cause harm, not its likelihood or severity. Impact describes how bad the outcome could be, but not how likely it is. Exposure refers to being open to threats, not the overall risk level. So the concept described by the question is risk.

SAMPLE

6. Which term refers to a security solution designed to manage and control cloud service usage across users and devices?

A. Credentialed scan

B. Vulnerability scanner

C. Cloud identity and access management

D. Cloud access security broker (CASB)

The term that fits this description is a Cloud Access Security Broker. A CASB sits between users and cloud services and provides visibility into which cloud apps are in use, who is using them, and from which devices. It enforces security policies across both sanctioned and unsanctioned cloud applications, giving you control over access, data protection (like DLP and encryption), and threat protection, while helping maintain compliance. This combination of visibility and policy enforcement across multiple users and devices is what sets CASB apart from the other options. A credentialed scan or a vulnerability scanner focuses on identifying weaknesses in systems, not governing cloud service usage. Cloud identity and access management handles authentication and access to cloud resources but doesn't inherently provide broad governance or control of cloud app usage across devices.

7. Which term refers to hardware or software used on a private network without the owner's knowledge?

A. Shadow IT

B. Unauthorized

C. Hacker

D. Internal threat

Shadow IT describes the practice of using hardware or software within an organization without the knowledge or approval of the owner or IT department. It happens when people bring in unsanctioned devices, install unapproved applications, or use cloud services without security oversight, effectively adding resources to a private network without being monitored. This hidden layer can create security gaps—like unpatched software, weak data protection, and untracked access—because it bypasses standard controls and monitoring. A hacker refers to a person who breaks into systems, which is not what's described here. An internal threat is about risk from someone inside the organization who misuses authorized resources. Unauthorized is a generic descriptor, but the established term for this phenomenon is Shadow IT, which specifically captures the unapproved usage of technology on the private network.

8. What security control enforces a virtual boundary based on real-world geography?

A. Geofencing

B. Geolocation-based access control

C. Geo-blocking

D. Geographic boundary enforcement

Geofencing creates a virtual boundary around real-world geography and enforces security policies based on whether a device or user is inside or outside that boundary. It uses location data from GPS, Wi Fi, or cellular signals to detect entry or exit and can trigger actions like granting or denying access, sending alerts, or altering app behavior. This direct mechanism—defining a geographic perimeter and enforcing rules as boundaries are crossed—is why it's the best fit for the question. Related ideas exist (for example, using location as a condition in access decisions or restricting content by region), but they do not describe the specific boundary-enforcement control that geofencing provides.

SAMPLE

9. Which term describes a guided, non-live exercise used to discuss response to events?

A. Drill

B. Live Exercise

C. Functional Test

D. Tabletop Exercises

Tabletop exercises are guided, non-live sessions where teams discuss how they would respond to a hypothetical incident. A facilitator leads the scenario, prompts decision points, and participants walk through actions, communications, and escalation as if the event were unfolding, but no real systems are activated. This setup focuses on understanding roles, coordination, and decision-making rather than performing hands-on response. That's why it fits a guided, non-live exercise used to discuss how to react to events. In contrast, drills are hands-on practice of specific procedures, live exercises involve real-time actions and potential deployment of resources, and functional tests verify that a particular system function behaves correctly.

10. Which architectural style is described as stateless and uses standard operations for web services?

A. GraphQL

B. SOAP

C. REST

D. RPC

Statelessness and the use of standard HTTP operations describe RESTful web services. In REST, each request contains all the information needed to complete it, and the server does not rely on stored session context between requests. Interactions revolve around resources identified by URIs, with operations mapped to the standard HTTP methods like GET, POST, PUT, and DELETE, making the interface uniform and easily cacheable. GraphQL differs by using a flexible query language over a single endpoint rather than a set of standard HTTP actions; SOAP is a protocol with a fixed envelope and actions defined in WSDL; RPC emphasizes invoking procedures rather than manipulating resources. Because it embodies statelessness and standard HTTP operations, REST best matches the description.

SAMPLE

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!

SAMPLE