Information Security Principles and Frameworks Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

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 governance practice ensures each asset has a clearly identified owner and is properly tagged within the inventory?

A. Assignment/Accounting

B. Data Historian

C. IoT

D. Zero Trust

2. Classifying the ownership and management of a cloud as public, private, community, or hybrid describes what concept?

A. cloud deployment model

B. cloud service model

C. cloud deployment model

D. virtualization model

3. Signatures and pattern-matching rules supplied to analysis platforms as an automated feed.

A. Reputational threat intelligence

B. cyber threat intelligence (CTI)

C. threat feeds

D. software bill of materials (SBOM)

4. Which term defines historical analysis of cyber attacks and the actions of adversaries?

A. Forensics

B. Threat modeling

C. Tactics, techniques, and procedures (TTPs)

D. MITRE ATT&CK

5. Which term denotes a monitor that sniffs data from frames as they traverse network media?

A. TAP

B. Sensor

C. Inline

D. SPAN

6. A number used with authentication devices such as smart cards; the PIN should be known only to the user, loss of the smart card should not present a security risk.

A. password manager

B. account policies

C. personal identification number (PIN)

D. multifactor authentication

7. In a Wi-Fi site survey, what diagram shows signal strength and channel utilization at different locations?

A. Heat map

B. Signal diagram

C. Coverage map

D. Location heat chart

8. Which personal authentication method was introduced with WPA3 to address vulnerabilities in WPA-PSK?

A. WPS

B. Simultaneous Authentication of Equals (SAE)

C. PSK

D. EAP-TLS

9. Which software delivery model streams code that runs on a server and is delivered to a client?

A. Application virtualization

B. Platform as a Service

C. Infrastructure as a Service

D. Software as a Service

10. Which term describes the ability of a system to scale with increasing demand?

A. MAC filtering

B. Compute

C. air-gapped

D. Scalability

Answers

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

Explanations

1. Which governance practice ensures each asset has a clearly identified owner and is properly tagged within the inventory?

A. Assignment/Accounting

B. Data Historian

C. IoT

D. Zero Trust

Assigning ownership and tagging assets in the inventory creates clear accountability and traceability. When every asset has a designated owner, there's a responsible party for its lifecycle, security, and compliance. Tagging provides a reliable way to identify and locate the asset in the register, enabling accurate tracking, audits, and incident responses. Together, these practices keep the asset inventory accurate and up to date, which is essential for governance and risk management. Other concepts don't directly address who owns an asset or how it is labeled in the inventory: a Data Historian collects and stores historical data from devices, not asset ownership; IoT refers to connected devices and networks, not governance of asset records; Zero Trust is a security model about verifying access, not managing asset ownership and tagging.

2. Classifying the ownership and management of a cloud as public, private, community, or hybrid describes what concept?

A. cloud deployment model

B. cloud service model

C. cloud deployment model

D. virtualization model

The concept being tested is how cloud resources are owned and managed, which is defined by cloud deployment models. Public cloud means the infrastructure is owned by a cloud provider and offered to the general public, with resources shared among many tenants. Private cloud is dedicated to a single organization, often on its own premises or in a privately managed environment, giving more control and security. Community cloud is shared by multiple organizations with common concerns, while hybrid cloud combines two or more deployment models to allow data and workload movement between them. This classification focuses on ownership and management of the infrastructure, not on the services being consumed. Service models (IaaS, PaaS, SaaS) describe what is provided, not who owns the infrastructure, and virtualization is a technology used across deployment models, not a deployment model itself. Therefore, the correct concept is cloud deployment model.

3. Signatures and pattern-matching rules supplied to analysis platforms as an automated feed.

A. Reputational threat intelligence

B. cyber threat intelligence (CTI)

C. threat feeds

D. software bill of materials (SBOM)

Threat feeds are automated data streams that deliver indicators of compromise, detection signatures, and rule sets to security platforms so they can automatically detect known threats. When signatures and pattern-matching rules are provided as an automated feed to analysis platforms, it's describing a threat feed—the mechanism that keeps detection engines up to date with the latest detection logic and patterns to look for in data, files, or network traffic. This is different from reputational threat intelligence, which focuses on the trustworthiness or maliciousness of entities like domains or IPs rather than the actual detection rules. It's also broader than CTI, which covers contextual information about threat actors, campaigns, techniques, and vulnerabilities, not just the automated delivery of detection signatures. Finally, an SBOM lists software components and their dependencies, licenses, and supply-chain details, not security detection rules.

4. Which term defines historical analysis of cyber attacks and the actions of adversaries?

A. Forensics

B. Threat modeling

C. Tactics, techniques, and procedures (TTPs)

D. MITRE ATT&CK

TTPs, or Tactics, Techniques, and Procedures, are the patterns of attacker behavior across cyber campaigns. When you analyze historical cyber attacks, you're looking at the tactics adversaries aimed for, the techniques they used to accomplish them, and the specific procedures or tools they employed along the way. This way of thinking lets you summarize how attackers operate, compare incidents, and anticipate how similar campaigns might unfold in the future. MITRE ATT&CK is a framework that catalogs these TTPs to help analysts map observed actions to a standardized set of behaviors, but the concept you're identifying is the TTPs themselves—the description of how adversaries act. Forensics deals with collecting and examining evidence from a single incident, while threat modeling focuses on identifying potential threats and designing defenses in advance.

5. Which term denotes a monitor that sniffs data from frames as they traverse network media?

A. TAP

B. Sensor

C. Inline

D. SPAN

The main idea is how traffic is observed for security monitoring. A sensor is the component that actively captures and inspects the frames as they travel over network media, serving as the monitoring device in a security system. It collects packets, analyzes content or metadata, and provides data to analysis tools for detection and investigation. A TAP is a passive device that splits the signal to give a monitoring point without interfering with traffic; SPAN copies traffic within a switch to a monitoring port; Inline describes placing a device directly in the data path, which can affect traffic and is about placement rather than the act of sniffing. Because the question describes a monitor that sniff data from frames as they traverse the network, the sensor best fits that role.

6. A number used with authentication devices such as smart cards; the PIN should be known only to the user, loss of the smart card should not present a security risk.

A. password manager

B. account policies

C. personal identification number (PIN)

D. multifactor authentication

A PIN is a secret number that serves as a knowledge factor used with a physical token like a smart card. The card provides the possession factor, and the PIN ensures you must know something to use the card. Because the PIN is known only to the user, losing the card doesn't automatically grant access—the attacker would still need the PIN to operate the card. This is why the PIN fits the scenario best: it's the private number that accompanies the smart card to authenticate the user. A password manager isn't the secret used with a card; it stores credentials. Account policies describe rules and controls, not a personal secret used for authentication. Multifactor authentication is the overall approach of requiring multiple factors, but the scenario specifically describes the secret number that unlocks the card.

7. In a Wi-Fi site survey, what diagram shows signal strength and channel utilization at different locations?

A. Heat map

B. Signal diagram

C. Coverage map

D. Location heat chart

Visualizing how signal strength varies across a site is shown with a heat map. In a Wi-Fi site survey, a heat map maps measurements of signal strength (and often channel utilization) to specific locations, using color intensity to indicate stronger or weaker coverage. This makes it easy to spot dead zones, overlap, and congested channels, guiding where to place access points or adjust channels. A coverage map is broader and doesn't always convey the detailed gradient of signal strength and usage across the space. The other terms aren't standard outputs for this purpose. So the diagram that best communicates signal strength and channel utilization at different locations is the heat map.

8. Which personal authentication method was introduced with WPA3 to address vulnerabilities in WPA-PSK?

A. WPS

B. Simultaneous Authentication of Equals (SAE)

C. PSK

D. EAP-TLS

SAE, or Simultaneous Authentication of Equals, is the password-based handshake used in WPA3 for personal networks. It replaces the static pre-shared key approach of WPA-PSK with a mutual authentication method that never exposes the password and derives a fresh session key for each connection. This design makes offline password guesses much harder: an attacker capturing handshakes cannot simply try guesses against a stored key, because the handshake involves ephemeral values and a Dragonfly-style exchange that requires interactive participation from both sides. The result is mutual authentication and forward secrecy, so even if a password is weak, past sessions aren't compromised if the password or keys are later exposed. WPS is a setup convenience feature with known vulnerabilities, not the authentication method introduced with WPA3. PSK refers to the older static pre-shared key approach used in WPA/WPA2-PSK, which is precisely what SAE was designed to improve upon. EAP-TLS is an enterprise authentication method using certificates, not the WPA3 personal mechanism.

9. Which software delivery model streams code that runs on a server and is delivered to a client?

A. Application virtualization

B. Platform as a Service

C. Infrastructure as a Service

D. Software as a Service

Delivering software where the code runs on a server and is streamed to a client describes application virtualization, often called remote app streaming. In this approach, the application executes on a central server, and the user interacts with a streamed interface on their device. This lets you run the program without installing it locally and keeps processing centralized. Platform as a Service provides environments for developers to build and deploy applications, not primarily about streaming a finished app to end users. Infrastructure as a Service offers virtualized hardware resources, while Software as a Service delivers a complete application hosted on servers and accessed over the network; the emphasis there is on usage over the web rather than streaming the app's executable interface to a client.

10. Which term describes the ability of a system to scale with increasing demand?

A. MAC filtering

B. Compute

C. air-gapped

D. Scalability

Scaling with increasing demand is scalability—the system's ability to grow capacity or performance as workload rises without a drop in service quality. In practice this means architectural choices like adding more servers (horizontal scaling), upgrading hardware (vertical scaling), using load balancing, caching, and auto-scaling in cloud environments. This term is the best fit because it directly describes a system's capability to handle higher demand. The other options fail to capture this property: MAC filtering is a security control that restricts access by device MAC address and doesn't address how the system handles more load; Compute refers to processing power or work to be done and isn't about the system's ability to scale; air-gapped means a network is physically isolated for security and has nothing to do with scaling resources.

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!