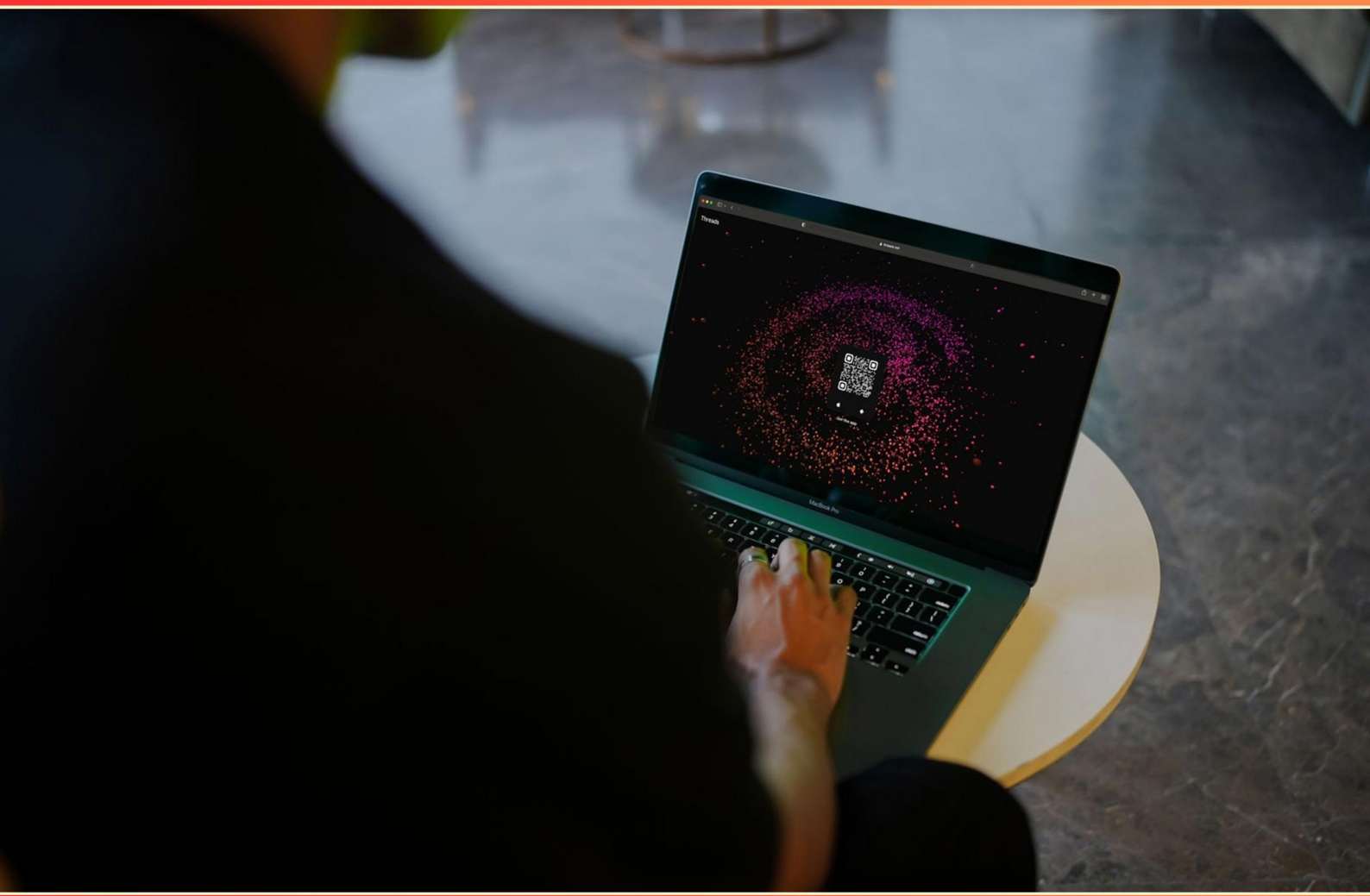
COMPTIA SECURITYX PRACTICE TEST (SAMPLE)

STUDY GUIDE



Prepare with structure. Pass with confidence

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. What term is defined as a site that is up and running continuously?

A. Hash

B. External Actors

C. Hot Site

D. Informative Policies

2. Which agreements are binding and used to govern ongoing operations between partners?

A. Interoperability Agreements

B. Memorandum of Understanding (MOU)

C. Business Impact Analysis (BIA)

D. Third-Party Connection Agreement (TCA)

3. Which term is used to force compliance with the security policy and practices within the organization?

A. Deterrent Control

B. Directive Control

C. Detective Control

D. Preventive Control

4. Which term describes the process of reducing a device's attack surface by disabling unused features, services, or ports?

A. End of Support (EOS)

B. Device Hardening

C. Containerization (Mobile)

D. eFuse

5. What metric represents the average amount of time it would take to repair an asset or component after a disaster?

A. Mission Essential Functions (MEFs)

B. Mean Time to Repair (MTTR)

C. Recovery Service Level (RSL)

D. Privacy Impact Assessment (PIA)

SAMPLE

6. Occurs when a part of a company is 'spun off' to form its own company.

A. Merger

B. Divestiture/Demerger

C. Acquisition

D. Spin-off

7. Which tool provides granular control to allow or disallow inheritance of a policy from one group or container to another?

A. Air Gap

B. Region-Based Segmentation

C. Data Zone

D. Group Policy Management Console (GPMC)

8. Which component stores usernames, passwords, or encryption keys?

A. Credential Management

B. Password Policies

C. Hardware Key Manager

D. Complexity

9. Which element provides the memory and processing functions between devices and the agents?

A. Managed Device

B. Break and Inspect

C. Network Management Station (SNMP Manager)

D. SIEM Systems

10. To ensure an application can be deployed across Azure, AWS, and Google Cloud, which risk is addressed?

A. Application Transfer Risk

B. Infrastructure Transfer Risk

C. Human Resource Knowledge Risk

D. Vendor Lock-out

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What term is defined as a site that is up and running continuously?

A. Hash

B. External Actors

C. Hot Site

D. Informative Policies

A hot site is a fully provisioned alternate facility that remains up and running continuously so you can switch operations with minimal downtime after a disruption. In disaster recovery and business continuity, this means the site has hardware, software, network connectivity, and often data mirrors already in place, ready to take over immediately if the primary site fails. This setup minimizes interruption to operations and data loss, which is why it's described as continually ready to operate. For contrast, a hash is a cryptographic function used to verify data integrity, external actors are potential attackers, and informative policies are security guidelines. Those concepts don't describe a ready-to-activate recovery site, so they're not the term that fits this scenario.

2. Which agreements are binding and used to govern ongoing operations between partners?

A. Interoperability Agreements

B. Memorandum of Understanding (MOU)

C. Business Impact Analysis (BIA)

D. Third-Party Connection Agreement (TCA)

Interoperability agreements establish binding terms that govern how partners work together over time. They spell out responsibilities, data exchange formats, interfaces, security controls, incident response, and change management, creating enforceable obligations that ensure systems from different organizations continue to operate together smoothly. This makes them the best fit for governing ongoing operations between partners, because they provide a formal framework your teams must follow day to day. A memorandum of understanding, by contrast, is typically non-binding and outlines intent or general cooperation rather than enforceable duties. A business impact analysis is a planning activity that assesses potential effects of disruptions, not a governance contract. A third-party connection agreement describes a specific connection arrangement but does not universally govern ongoing collaboration between partners in the broader sense.

3. Which term is used to force compliance with the security policy and practices within the organization?

A. Deterrent Control

B. Directive Control

C. Detective Control

D. Preventive Control

Directive controls are administrative measures that mandate actions to comply with security policy. They force consistent behavior by establishing requirements, roles, and processes that people must follow—such as security policies, standards, procedures, and mandatory training. This is why they best describe forcing compliance: they set explicit expectations and consequences for noncompliance, guiding how the organization and its members should operate. Deterrent controls aim to discourage violations through penalties or warnings but don't compel action. Detective controls identify and reveal violations after they occur, rather than enforcing the policy in real time. Preventive controls try to stop incidents from happening in the first place, by limiting access or capabilities.

SAMPLE

4. Which term describes the process of reducing a device's attack surface by disabling unused features, services, or ports?

A. End of Support (EOS)

B. Device Hardening

C. Containerization (Mobile)

D. eFuse

Reducing a device's attack surface by turning off unused features, services, or ports is called device hardening. The idea behind hardening is that every active service or open port can be a potential entry point for an attacker, so removing unnecessary capabilities lowers the number of ways a system could be compromised. Practical steps include disabling services and protocols that aren't needed, closing unused network ports, removing unused apps, applying secure configuration baselines, and enforcing least-privilege access. This is an ongoing practice tied to keeping an accurate asset inventory, applying patches, and maintaining secure defaults. For context, End of Support means a vendor no longer provides updates for a product, which doesn't describe actively reducing exposure. Containerization isolates applications but doesn't inherently reduce the device's attack surface—instead, it changes how software runs. An eFuse is a hardware fuse used to store permanent security states, not a method for reducing attack surface through configuration.

5. What metric represents the average amount of time it would take to repair an asset or component after a disaster?

A. Mission Essential Functions (MEFs)

B. Mean Time to Repair (MTTR)

C. Recovery Service Level (RSL)

D. Privacy Impact Assessment (PIA)

The main idea is understanding how we measure downtime during recovery. The metric that captures the average time it would take to repair an asset or component after a disaster is Mean Time to Repair. MTTR reflects the typical duration from when a fault or failure is detected to when the asset is repaired and back in operation, including the steps of diagnosis, repair work, testing, and handover. This measure helps teams plan for outages, set realistic downtime expectations, and identify bottlenecks in the repair process so recovery efforts can be improved. Other terms describe different concepts: Mission Essential Functions focus on the critical operations that must continue rather than how long repairs take; Recovery Service Level defines the target time to restore services but isn't the actual repair duration; Privacy Impact Assessment evaluates privacy risks, not repair timing.

6. Occurs when a part of a company is 'spun off' to form its own company.

A. Merger

B. Divestiture/Demerger

C. Acquisition

D. Spin-off

Spun off describes creating a new, independent company from part of the existing business and distributing shares of that new company to the current shareholders. That exact mechanism—forming a separate entity from a portion of the original company and handing shares to shareholders—defines a spin-off. It's different from a divestiture, which is selling the unit to another party, and from a demerger, which is simply splitting into separate entities (which may not involve issuing a new, independently owned company to shareholders). The use of "spun off" signals a spin-off action.

SAMPLE

7. Which tool provides granular control to allow or disallow inheritance of a policy from one group or container to another?

A. Air Gap

B. Region-Based Segmentation

C. Data Zone

D. Group Policy Management Console (GPMC)

Managing how policies flow between containers in Active Directory is about Group Policy inheritance, and the Group Policy Management Console is the tool that controls this flow. GPMC lets you view, link, and manage Group Policy Objects across domains, sites, and organizational units, giving you precise control over where a policy is applied. You can enable or block inheritance on a specific container, and you can enforce a GPO so its settings take precedence over others higher up in the hierarchy. This combination—linking policies to containers and adjusting how they inherit—provides the granular control described in the question. The other options don't fit this function. An Air Gap describes complete network isolation, which has nothing to do with how policies cascade. Region-Based Segmentation is about dividing a network into segments, not about policy inheritance. Data Zone isn't a standard tool for managing policy inheritance.

8. Which component stores usernames, passwords, or encryption keys?

A. Credential Management

B. Password Policies

C. Hardware Key Manager

D. Complexity

Storing usernames, passwords, and encryption keys requires a dedicated, tamper-resistant storage and processing component that isolates secrets from the rest of the system. A hardware key manager is built to do exactly that: it keeps credentials and cryptographic keys in hardware, protecting them from exposure in memory, logs, or software layers. It can generate keys, securely store them, enforce who can access them, and perform cryptographic operations inside the device, which helps prevent keys from being stolen or misused. The other terms describe practices or rules rather than a secure storage facility. Credential management covers the overall handling of credentials across systems, not the physical protection of the secrets. Password policies specify how passwords should be created and managed, and complexity refers to an attribute of passwords rather than a storage mechanism. So the hardware key manager best fits the need to securely store usernames, passwords, or encryption keys.

SAMPLE

9. Which element provides the memory and processing functions between devices and the agents?

A. Managed Device

B. Break and Inspect

C. Network Management Station (SNMP Manager)

D. SIEM Systems

In SNMP architecture, the central element that handles management tasks, stores data, and processes information from many devices is the network management station (the SNMP manager). Devices run SNMP agents that collect status and performance data and respond to the manager's requests. The manager coordinates polling, collects the data, and performs the processing needed to monitor and manage the network. That central processing and memory resource located in the manager is why it's the best answer. The other options describe different roles: a managed device is the device being managed and hosts the agent but doesn't serve as the central processing hub; Break and Inspect refers to inline traffic inspection at a chokepoint, not SNMP management; and SIEM systems gather and analyze security events from across the network, which is about security event correlation rather than the standard management interface between devices and their agents.

10. To ensure an application can be deployed across Azure, AWS, and Google Cloud, which risk is addressed?

A. Application Transfer Risk

B. Infrastructure Transfer Risk

C. Human Resource Knowledge Risk

D. Vendor Lock-out

The main idea here is portability—the ability to move and run the same application across different cloud environments without major rewrites. When you design and package an app so it can be deployed on Azure, AWS, and Google Cloud, you're addressing the risk that the application cannot be transferred to another cloud easily. This is known as application transfer risk. You reduce it by using portable approaches: containerize the app so it runs consistently wherever it's hosted, rely on provider-agnostic services and standard interfaces, and manage infrastructure with cloud-agnostic tooling and declarative, portable configurations. That way, the application can be redeployed across clouds with minimal changes, instead of being tied to a single provider's unique features.

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://comptiasecurityx.examzify.com

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

SAMPLE