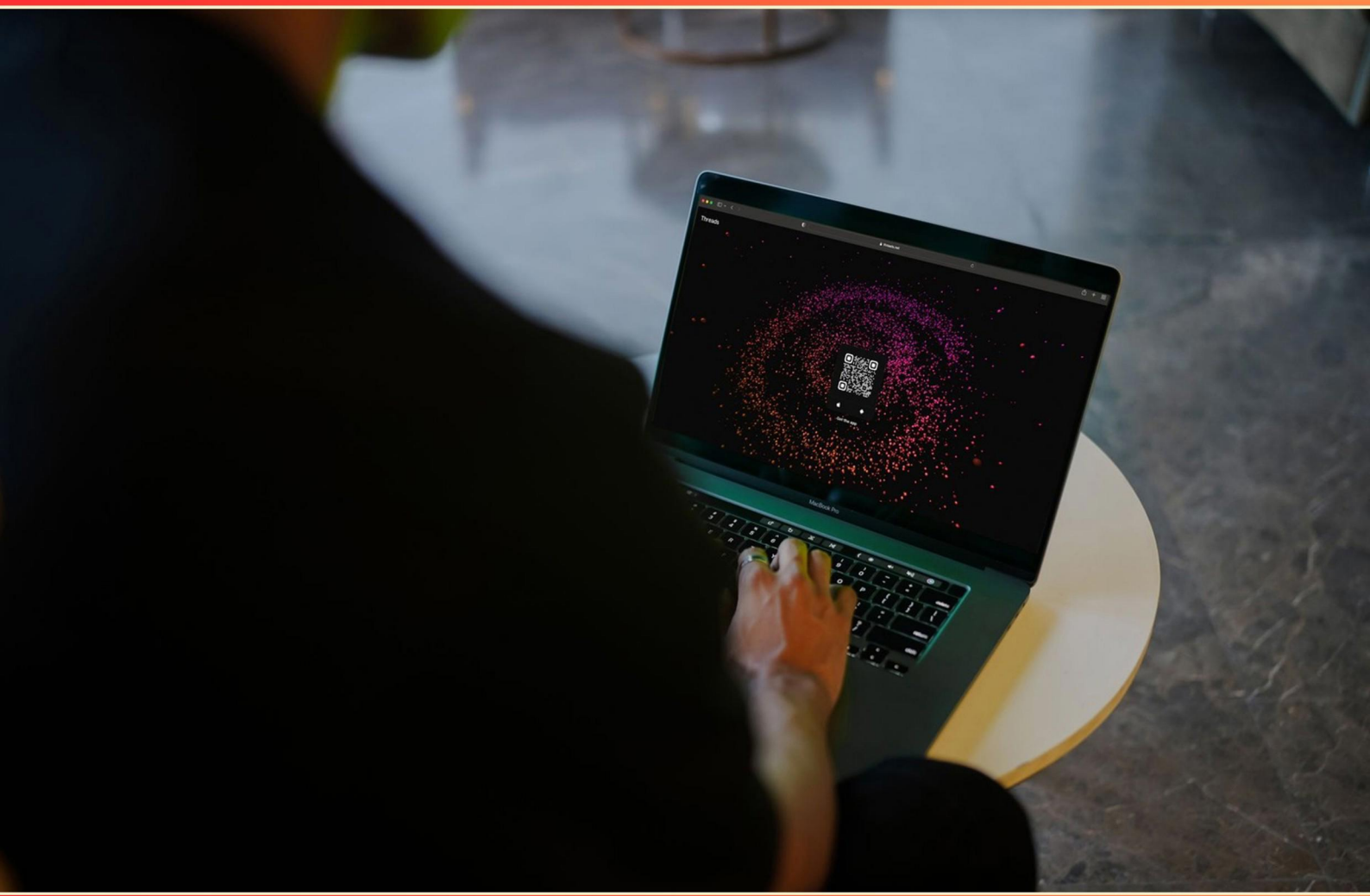
COMPTIA SECURITYX PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://comptiasecurityx.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 term captures the same information as a baseline but at a different point in time?**

   A. Benchmark

   B. Latency

   C. KRI

   D. KPI

2. **Which process identifies and manages privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, business relationships, and other risk events?**

   A. Mission Essential Functions (MEFs)

   B. Mean Time to Repair (MTTR)

   C. Recovery Service Level (RSL)

   D. Privacy Impact Assessment (PIA)

3. **Which term describes the risk that remains after applying mitigations and security controls?**

   A. Inherent Risk

   B. Residual Risk

   C. Control Risk

   D. Operational Risk

4. **If a system blocks data movement based on classification levels, which feature is being used?**

   A. Dictionary

   B. Quarantine

   C. RDP Blocking

   D. Classification-Based Data Blocking

5. **Which term describes large or complex data sets that traditional data processing applications cannot sufficiently handle?**

   A. Cryptocurrency

   B. Big Data

   C. Blockchain

   D. Distributed Consensus

SAMPLE

6. During an outage, if the system is required to receive payments and provide services, which loss occurs?

A. Loss of Productivity

B. Loss of Revenue

C. Revenue Interruption

D. Payment Delay

7. Which security system scans network traffic for malicious activity and can stop it?

A. Wireless IDS (WIDS)

B. Network Access Control (NAC)

C. Intrusion Prevention System (IPS)

D. Secure Shell (SSH)

8. Which mechanism focuses on securing accounts with elevated privileges and monitoring their activity?

A. Privileged Access Management

B. Credential Management

C. Hardware Key Manager

D. Password Policies

9. Which term describes a microprocessor manufacturing utility that is part of a validated supply chain?

A. CAM Table

B. Trusted Foundry

C. Source Authenticity

D. Port Security

10. Which term describes data lost after power loss?

A. Persistent

B. Non-Persistent

C. High Availability

D. Replication

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which term captures the same information as a baseline but at a different point in time?

A. Benchmark

B. Latency

C. KRI

D. KPI

Using a reference point in time to compare performance. A baseline records the initial state at a specific moment. When you want to assess how things look at a different moment while keeping the same kind of information, you use a benchmark—a reference point for comparison over time or against standards. So it captures the same information as a baseline but anchored at another point in time, making it the best fit. Latency is about delay, a KRI signals potential risk, and a KPI tracks progress toward objectives.

2. Which process identifies and manages privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, business relationships, and other risk events?

A. Mission Essential Functions (MEFs)

B. Mean Time to Repair (MTTR)

C. Recovery Service Level (RSL)

D. Privacy Impact Assessment (PIA)

A privacy risk assessment is a structured process used when planning new projects, systems, processes, policies, or business relationships to identify and manage privacy risks. It looks at how personal data is collected, used, shared, stored, and retained, and it evaluates whether current safeguards are enough or if additional controls are needed. This involves considering applicable laws and regulations, data minimization, access controls, data subject rights, and potential impacts to individuals. The outcome is a documented assessment that describes the privacy risk levels and a plan of mitigations—so the project can proceed with privacy protections in place. Other concepts in the options focus on maintaining essential operations, repair metrics, or recovery targets, not on identifying and addressing privacy risks, which is the distinct purpose of a privacy risk assessment.

3. Which term describes the risk that remains after applying mitigations and security controls?

A. Inherent Risk

B. Residual Risk

C. Control Risk

D. Operational Risk

The risk that remains after applying mitigations and security controls is residual risk. After identifying the inherent risk—the level of threat exposure before any safeguards—you implement measures to reduce it. The portion that still exists after those safeguards is what you monitor and manage as residual risk. For example, even with encryption and access controls in place, there may still be a small chance of a breach; that remaining chance is residual risk. This differs from inherent risk (risk before controls), operational risk (risks in day-to-day operations), and any term that would describe risk caused by controls themselves failing.

SAMPLE

4. If a system blocks data movement based on classification levels, which feature is being used?

A. Dictionary

B. Quarantine

C. RDP Blocking

D. Classification-Based Data Blocking

Data movement is governed by data loss prevention policies that use data classifications to control where information can go. When data is labeled with a classification level (such as confidential or restricted), a policy can block its transfer to destinations or channels that aren't permitted for that level. This approach—enforcing actions based on the data's classification label—is classification-based data blocking. It's a data-centric security measure that stops sensitive information from leaving the environment according to the policy. The other options don't fit this scenario: a dictionary approach relies on matching terms inside content, not on predefined classification labels; quarantine isolates items after detection but doesn't enforce blocking based on classification levels; and blocking RDP stops a type of network traffic rather than enforcing data movement rules based on data classification.

5. Which term describes large or complex data sets that traditional data processing applications cannot sufficiently handle?

A. Cryptocurrency

B. Big Data

C. Blockchain

D. Distributed Consensus

Big data describes data sets that are too large or complex for traditional data processing tools to handle efficiently. This challenge often involves the three Vs: volume (massive amounts of data), velocity (rapid data inflow requiring real-time or near-real-time processing), and variety (diverse data types and formats, including unstructured data). Traditional systems are typically designed for smaller, structured data and batch processing, so they struggle with storage, processing speed, and integration when faced with big data. To manage these demands, organizations use scalable, distributed storage and processing frameworks that can run across many machines, enabling timely analysis and insights from vast datasets. The other terms relate to different concepts: cryptocurrency is a digital currency, blockchain is a distributed ledger technology, and distributed consensus is a method for agreeing on state in a distributed system; none describe the overarching challenge of handling extremely large or complex data sets.

6. During an outage, if the system is required to receive payments and provide services, which loss occurs?

A. Loss of Productivity

B. Loss of Revenue

C. Revenue Interruption

D. Payment Delay

When a system that handles payments and delivers services is down, the immediate effect is that money that would have been earned isn't collected. This is a direct financial impact: the business experiences a loss of revenue because transactions can't be completed and value can't be delivered during the outage. Payment delays can occur, but they describe a timing issue rather than the overall amount that's not earned. Revenue interruption is a similar concept, yet the phrasing "loss of revenue" emphasizes the actual reduction in income for that downtime. Productivity losses relate to internal efficiency and don't capture the primary missed revenue from unavailable services.

SAMPLE

7. Which security system scans network traffic for malicious activity and can stop it?

A. Wireless IDS (WIDS)

B. Network Access Control (NAC)

C. Intrusion Prevention System (IPS)

D. Secure Shell (SSH)

The idea here is real-time defense that sits in the traffic path and both detects and blocks threats. An Intrusion Prevention System is placed inline on the network so it can inspect packets as they travel by. It looks for known attack signatures and unusual behavior, and when it finds something malicious it can take immediate action—dropping the offending packets, resetting connections, or blocking traffic from the source. That active blocking is what makes it different from detection-only systems: it doesn't just alert; it stops the attack in real time. WIDS focuses on wireless traffic, not general network traffic. NAC enforces device posture and access control, which helps keep untrusted devices out or limited, but it doesn't continuously scan and block malicious activity in the flow of traffic. SSH is simply a secure remote access protocol, not a system for monitoring or blocking traffic.

8. Which mechanism focuses on securing accounts with elevated privileges and monitoring their activity?

A. Privileged Access Management

B. Credential Management

C. Hardware Key Manager

D. Password Policies

Privileged Access Management focuses on protecting accounts with elevated privileges and tracking their activity. These accounts can unlock many systems and data, so they're prime targets for attackers and insiders. PAM solutions vault and rotate privileged credentials, enforce just-in-time access, require strong authentication, and monitor and audit privileged sessions to detect unusual activity and enforce accountability. This combination of credential control and ongoing monitoring is what makes PAM the best fit for securing high-privilege accounts. The other options are broader or unrelated: credential management covers handling credentials in general without specific emphasis on privileged sessions; hardware key managers deal with cryptographic keys stored in hardware; and password policies set rules for passwords but don't focus on privileged access monitoring.

SAMPLE

9. Which term describes a microprocessor manufacturing utility that is part of a validated supply chain?

A. CAM Table

B. Trusted Foundry

C. Source Authenticity

D. Port Security

A trusted foundry refers to a semiconductor fabrication facility that has been vetted and approved to operate as part of a validated supply chain. The idea is that this kind of facility follows stringent security controls, governance, and traceability measures so the microprocessors it produces can be trusted not to be tampered with or contaminated by counterfeit parts. This trust in the manufacturing environment covers processes, equipment, personnel, and handling throughout fabrication, testing, and packaging, providing assurance about provenance and integrity of the chips. Other terms don't fit this context. A CAM table is about mapping MAC addresses to switch ports, not about manufacturing security or supply chain validation. Port security is a network feature that restricts devices on a switch port, again unrelated to where or how chips are made. Source authenticity isn't a standard descriptor for a manufacturing facility in this setting. So the concept best describing a microprocessor manufacturing utility within a validated supply chain is a trusted foundry.

10. Which term describes data lost after power loss?

A. Persistent

B. Non-Persistent

C. High Availability

D. Replication

Data that is lost after power loss comes from volatile memory, which doesn't survive a shutdown. This type of data is described as non-persistent. Non-persistent means the information disappears when power is removed, like what you'd expect from RAM or in-memory caches that aren't saved to non-volatile storage. In contrast, persistent data is stored to non-volatile media such as hard drives or SSDs and remains after power is restored. High availability focuses on keeping systems up and reachable with redundancy, not on whether individual data survives a power loss. Replication involves copying data to other locations for durability or disaster recovery, again not directly about whether data endures power loss.

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