NOCTI CYBERSECURITY STANDARD CERTIFICATION PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://nocticybersecstandard.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 security property ensures information and systems are accessible to authorized users when needed?

A. Availability

B. Confidentiality

C. Integrity

D. Non-repudiation

2. Which term describes enforcing access rights after authentication?

A. Authorization

B. Authentication

C. Access Control Lists

D. Multi-factor authentication

3. What activity represents regular preventive maintenance for security software?

A. Updating / patching to the latest versions of antivirus software

B. Turning off automatic updates

C. Installing only one antivirus on the network

D. Disabling firewall

4. In a cloud environment, which portion is typically handled by the customer in the shared responsibility model?

A. All infrastructure

B. Networking hardware

C. Data and configurations

D. Physical security of facilities

5. What is the role of TLS in data security?

A. TLS compresses and stores data at rest on servers.

B. TLS is a hardware device that blocks malware.

C. TLS provides encryption and integrity for data in transit between endpoints.

D. TLS replaces the need for authentication.

SAMPLE

6. Which CIA triad property ensures data integrity by preventing modification without authorization?

A. Availability

B. Integrity

C. Confidentiality

D. Authentication

7. Which security control allows access to a website for an individual or user group?

A. Whitelisting

B. Blacklisting

C. Cryptography

D. Transposition Cipher

8. Which term means integrating all three concepts of confidentiality, integrity, and availability into security planning?

A. CIA Triad

B. RBAC

C. DAC

D. Zero Day

9. Which cipher uses a grid-based system to substitute letters with symbol fragments?

A. Pigpen Cipher

B. Caesar Cipher

C. One Time Pad

D. Asymmetric encryption

10. What is the primary function of a firewall in network security?

A. To encrypt data traveling across networks.

B. To filter and monitor traffic between networks according to defined rules.

C. To route traffic based on IP addresses.

D. To provide end-user authentication.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which security property ensures information and systems are accessible to authorized users when needed?

A. Availability

B. Confidentiality

C. Integrity

D. Non-repudiation

Availability is the security property that ensures information and systems are accessible to authorized users when they need them. It means keeping services up and responsive, even in the face of failures or attacks, through redundancy, fault tolerance, backups, and good incident response. The goal is that legitimate users can reach the systems and data without unnecessary delays or interruptions. This differs from confidentiality, which focuses on preventing access by unauthorized people to data; integrity, which ensures data remains accurate and unaltered; and non-repudiation, which provides proof of origin and delivery to prevent denial of actions. For example, redundant servers and backup power help keep a website online during a failure, ensuring authorized users can still access the service.

2. Which term describes enforcing access rights after authentication?

A. Authorization

B. Authentication

C. Access Control Lists

D. Multi-factor authentication

Authorization is the process of granting or denying access based on permissions after identity has been established. Once someone proves who they are through authentication, the system checks what they're allowed to do and which resources they can reach. This decision is guided by roles, attributes, or policies, and it determines whether actions like reading, writing, or deleting a resource are permitted for that user. For instance, after logging in successfully, a user might be allowed to view a report but not to modify it, or to access only certain folders based on their role. Authentication is about proving identity, and multi-factor authentication is a method used during that proof. Access Control Lists describe specific permissions, but the act of applying those permissions to allow or block access is what authorization does.

3. What activity represents regular preventive maintenance for security software?

A. Updating / patching to the latest versions of antivirus software

B. Turning off automatic updates

C. Installing only one antivirus on the network

D. Disabling firewall

Regular preventive maintenance for security software means keeping the antivirus program up to date by applying updates and patches as they're released. When you update the software and its virus definitions, it can recognize and defend against newly discovered malware and close known security gaps in the program itself. This proactive maintenance helps ensure the protective layer remains effective against current threats and works well with other system updates. Other options don't fit this ongoing protection role: turning off automatic updates leaves the defenses exposed by missing important fixes and newer malware definitions; relying on only one antivirus on the network doesn't address consistent maintenance and can create gaps in protection; disabling the firewall removes a critical line of defense and is not a maintenance activity.

SAMPLE

4. In a cloud environment, which portion is typically handled by the customer in the shared responsibility model?

A. All infrastructure

B. Networking hardware

C. Data and configurations

D. Physical security of facilities

In the shared responsibility model, what the customer typically handles is data and configurations. The cloud provider takes care of the underlying infrastructure—physical hardware, networking gear, data center security, and the base platform. The customer is responsible for safeguarding the data they store in the cloud, including encryption, classification, retention, and backup, as well as configuring access controls, identity management, and the security settings of cloud services (such as firewall rules and secure default configurations). For example, you'd manage who can access data, what permissions they have, and how services are configured to enforce security policies, while the provider ensures the physical facilities, servers, storage, and virtualization are secure and up to date.

5. What is the role of TLS in data security?

A. TLS compresses and stores data at rest on servers.

B. TLS is a hardware device that blocks malware.

C. TLS provides encryption and integrity for data in transit between endpoints.

D. TLS replaces the need for authentication.

TLS protects data as it moves between two endpoints by encrypting it and ensuring its integrity, while also allowing the parties to verify each other's identities through certificates during the handshake. This combination keeps information confidential from eavesdroppers and makes sure that any tampering of the data is detected, so you know if a message has been altered in transit. It also supports authenticating the server (and optionally the client), which helps prevent man-in-the-middle attacks. TLS does not store data at rest, is not a hardware device, and does not replace authentication; it works with authentication to secure communications. So its primary role is encryption and integrity for data in transit between endpoints.

6. Which CIA triad property ensures data integrity by preventing modification without authorization?

A. Availability

B. Integrity

C. Confidentiality

D. Authentication

Integrity is the property that ensures information remains correct and unaltered by anyone who isn't authorized to change it. Preventing modifications without permission is the essence of integrity because any unauthorized change would undermine the trustworthiness of the data. To protect integrity, you put in place controls like strict access rights, audit logs to detect changes, and cryptographic measures such as hashes or digital signatures that verify data hasn't been tampered with. The other properties address different concerns: confidentiality focuses on keeping data private, availability ensures data is accessible when needed, and authentication verifies the identity of users or systems, not whether the data has been altered.

SAMPLE

7. Which security control allows access to a website for an individual or user group?

A. Whitelisting

B. Blacklisting

C. Cryptography

D. Transposition Cipher

Allowlisting controls access by explicitly listing who is allowed. A website can implement an allowlist to permit access only for specified individuals or groups, denying everyone else. When a user attempts to connect, the system checks the list and grants access if they're on it. This approach provides precise control over who can reach the site, which is ideal when access must be limited to particular people or roles, such as employees or partner organizations. In contrast, blacklisting blocks known bad actors but doesn't define who is allowed in general; cryptography and the transposition cipher are about protecting data through encryption rather than gatekeeping access to a site.

8. Which term means integrating all three concepts of confidentiality, integrity, and availability into security planning?

A. CIA Triad

B. RBAC

C. DAC

D. Zero Day

The main concept here is the CIA Triad, the foundational framing for security planning that integrates confidentiality, integrity, and availability. Confidentiality guards information so that only authorized people can access it, using controls like encryption and strict access management. Integrity ensures data is accurate and has not been tampered with, relying on measures such as checksums, digital signatures, and tamper-evident logging. Availability makes sure data and systems are accessible when needed, supported by redundancy, backups, and robust incident response. Thinking about security in terms of the CIA Triad means designing protections that simultaneously protect secrecy, trustworthiness, and uptime, rather than focusing on just one aspect. The other terms describe specific concepts without capturing that holistic integration: role-based access control concerns who is allowed to act on resources, discretionary access control is a permission model, and a zero-day refers to an unknown vulnerability.

9. Which cipher uses a grid-based system to substitute letters with symbol fragments?

A. Pigpen Cipher

B. Caesar Cipher

C. One Time Pad

D. Asymmetric encryption

This question tests recognizing a cipher by how it substitutes letters with symbol fragments drawn from a grid. The Pigpen cipher uses geometric grid patterns—typically two 3x3 grids (and two X-shaped grids)—to map each letter to a specific line segment or plus a dot to distinguish the second set. The result is letters replaced by visual fragments of the grid, not by ordinary letters. That's why this is the best choice: it's the classic example of grid-based substitution where symbols come from the grid's shapes rather than from a simple alphabetic shift or a key-based binary operation. In contrast, the Caesar cipher shifts letters along the alphabet, not via grid fragments; the One Time Pad produces ciphertext through a random key stream and modular addition rather than grid symbols; and asymmetric encryption uses public/private keys and distinct algorithms, not a fixed grid substitution.

SAMPLE

10. What is the primary function of a firewall in network security?

A. To encrypt data traveling across networks.

B. To filter and monitor traffic between networks according to defined rules.

C. To route traffic based on IP addresses.

D. To provide end-user authentication.

Firewalls filter and monitor traffic between networks based on defined rules. They act as a gatekeeper at the network boundary, inspecting data packets or connection flows and deciding whether to allow, block, or log them according to policy. This rule-driven control can rely on factors like source and destination addresses, ports, protocols, and sometimes the state of a connection, with stateful firewalls remembering ongoing conversations to enforce legitimate sessions. By doing so, they prevent unauthorized access while still permitting legitimate traffic and providing visibility through logs for monitoring and auditing. Other functions like encryption protect data contents, routing determines the path a packet takes, and authentication verifies user identity, but none of these primarily decide network access in the boundary where a firewall operates.

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://nocticybersecstandard.examzify.com

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

SAMPLE