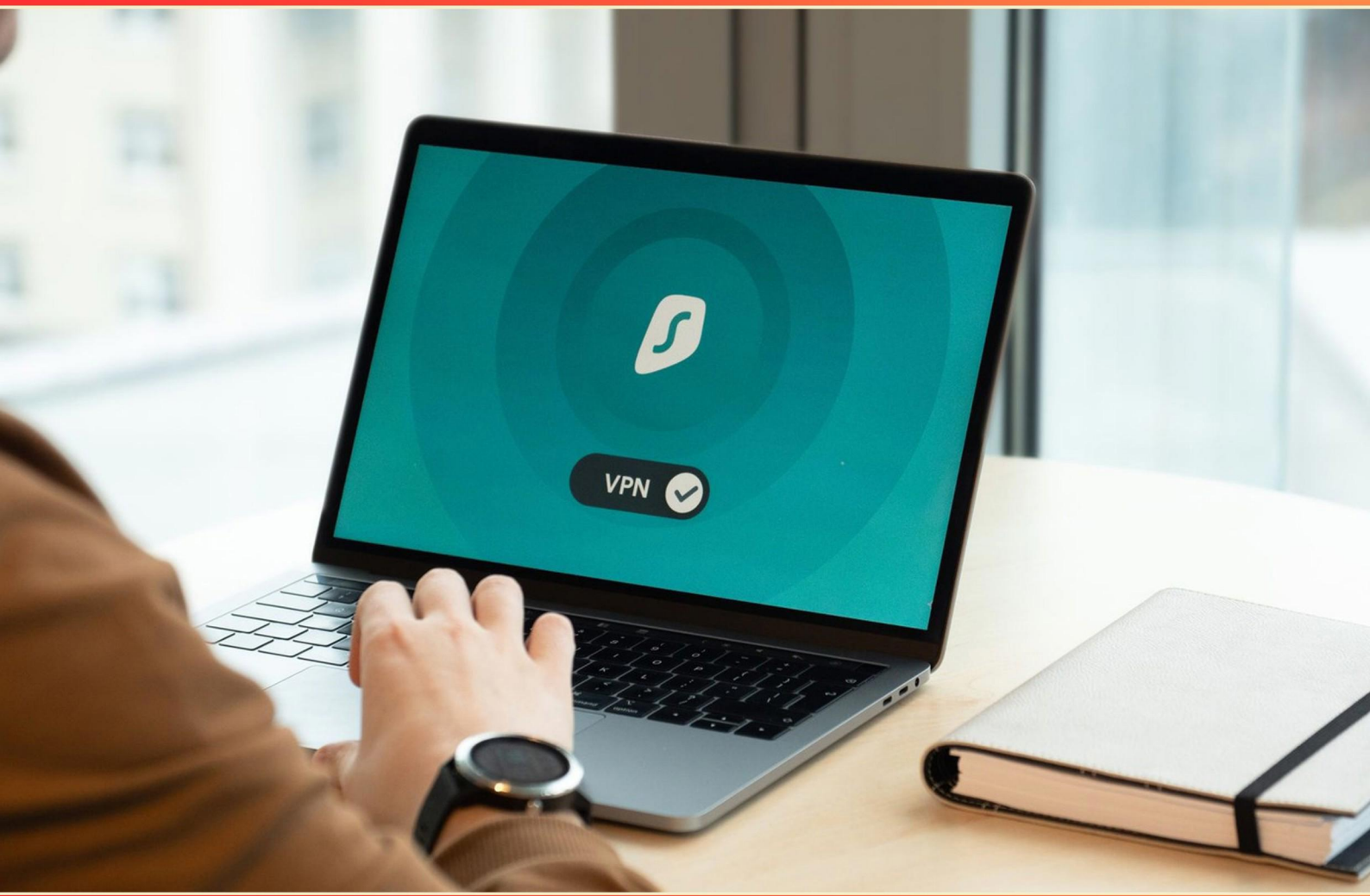
PCI DSS REQUIREMENTS PRACTICE TEST (SAMPLE)

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

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 statement about wildcards in PA-DSS is true?

A. They indicate major changes

B. They are the only variable element indicating minor, non-security changes

C. They have no meaning

D. They indicate security-critical fixes only

2. Which term describes the individual who purchases goods or services?

A. XSS

B. Database

C. Consumer

D. CSRF

3. System-level object refers to which of the following?

A. Anything on a system component required for its operation, including configuration files, libraries, drivers, and third-party components.

B. Only the hardware devices.

C. Only the system's network interfaces.

D. Only the operating system kernel.

4. An Audit Log provides a chronological record of system activities that enables what?

A. A non-reversible hash of data

B. Independently verifiable trail to reconstruct the sequence of events

C. Automatic data backup

D. Real-time intrusion detection

5. Which architecture best prevents direct public access from Internet to internal cardholder network components?

A. Direct Internet access to internal cardholder components is allowed if ports are closed.

B. The DMZ should be used to host all internal components.

C. Direct access is allowed via VPN.

D. Use a choke router and DMZ to ensure there is no direct access from the Internet to internal components.

SAMPLE

6. For shared hosting providers, what is required to protect hosted environments?

A. The hosting provider is solely responsible for customer PCI DSS compliance

B. Customers' data in hosted environments is not subject to PCI DSS

C. Shared hosting providers protect only the provider's own environment

D. The hosting provider must protect each entity's hosted environment and data; the customer entity must still comply with PCI DSS

7. Which statement correctly describes HTTPS?

A. It uses an insecure plain text channel.

B. It is HTTP over SSL/TLS, providing authentication and encryption for sensitive communications.

C. It is FTP over TLS for secure file transfer only.

D. It is a protocol for secure email transfer.

8. What is the primary objective of PCI DSS Requirement 1?

A. Establish a documented incident response plan.

B. Encrypt all data at rest.

C. Install & maintain a firewall configuration to protect cardholder data.

D. Monitor network activity continuously.

9. Which practice is commonly included to mitigate broken authentication and session management?

A. Exposing session IDs in the URL

B. Flagging session tokens as secure

C. Using a fixed, long-lived session ID for convenience

D. Disabling timeouts

10. ISO is described as which type of organization?

A. A governmental organization.

B. A non-governmental organization consisting of national standards institutes.

C. A private corporation.

D. An international regulatory body.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which statement about wildcards in PA-DSS is true?

A. They indicate major changes

B. They are the only variable element indicating minor, non-security changes

C. They have no meaning

D. They indicate security-critical fixes only

In PA-DSS, changes to a payment application are tracked and classified to determine if re-validation is needed. Wildcards are used specifically to indicate a minor, non-security change. This signaling is important because it helps assessors know that the update does not affect the security controls or data protection, and thus doesn't require the full re-validation path reserved for security changes. Since wildcards are the dedicated marker for these small, non-security updates, they are the only variable element used to signal this particular type of change. The other statements don't fit because wildcards do have meaning and aren't meant to flag major changes or security-critical fixes. Major changes and security-related fixes would be indicated in other ways and would typically trigger additional validation requirements.

2. Which term describes the individual who purchases goods or services?

A. XSS

B. Database

C. Consumer

D. CSRF

The main idea is identifying who buys goods or services in a transaction. The correct term is consumer, which describes the end user who purchases and uses goods or services. The other terms refer to things, not people: XSS is a web security vulnerability (Cross-Site Scripting), CSRF is another web attack (Cross-Site Request Forgery), and a database is a storage system for data. So, when asked who purchases goods or services, consumer is the exact label. In everyday shopping, you are the consumer, the seller is the merchant, and in PCI DSS contexts you might also see cardholder, but consumer fits this description best.

3. System-level object refers to which of the following?

A. Anything on a system component required for its operation, including configuration files, libraries, drivers, and third-party components.

B. Only the hardware devices.

C. Only the system's network interfaces.

D. Only the operating system kernel.

A system-level object includes anything on a system component that is required for its operation, spanning software and configuration, not just hardware. That's why the best answer covers configuration files, libraries, drivers, and third-party components—the full mix that a system relies on to function. The other options are too narrow: hardware devices alone don't account for software and config elements, network interfaces alone omit essential software layers, and the kernel alone ignores libraries, drivers, and configurations that also support operation. A practical example is a server that depends on the kernel, device drivers, shared libraries, and its configuration files to run correctly; all of these together constitute system-level objects.

SAMPLE

4. An Audit Log provides a chronological record of system activities that enables what?

A. A non-reversible hash of data

B. Independently verifiable trail to reconstruct the sequence of events

C. Automatic data backup

D. Real-time intrusion detection

An Audit Log is a chronological record of system activities that, when protected for integrity, provides an independently verifiable trail to reconstruct the sequence of events. This means you can trace who did what, when, and on which resources, and you can trust the order of those actions to investigate incidents, conduct audits, and meet compliance requirements. The emphasis is on the ability to verify and reconstruct events after they happen, not on backing up data or detecting intrusions in real time. A cryptographic or tamper evident approach helps ensure the log itself hasn't been altered, which is essential for trust in the reconstruction.

5. Which architecture best prevents direct public access from Internet to internal cardholder network components?

A. Direct Internet access to internal cardholder components is allowed if ports are closed.

B. The DMZ should be used to host all internal components.

C. Direct access is allowed via VPN.

D. Use a choke router and DMZ to ensure there is no direct access from the Internet to internal components.

Preventing direct exposure of the cardholder data environment to the Internet relies on placing a buffer between public networks and the sensitive systems and routing all access through a controlled point. A DMZ acts as that buffer, hosting only services that must be reachable from the Internet while keeping the core cardholder components behind stronger controls. A choke router creates a single chokepoint so all traffic from the Internet passes through a known, inspectable path, allowing precise firewall rules and logging before anything reaches internal components. This layered setup minimizes the attack surface and provides clear, enforceable boundaries, which is the strongest protection for PCI DSS requirements. Direct Internet access to internal components—even with ports supposedly closed—can be compromised through misconfigurations, new services, or overlooked paths. Placing all internal components in the DMZ would unnecessarily expose sensitive systems to the Internet. Direct access via VPN can be a legitimate way to enable remote work, but it still establishes a path from the Internet into internal resources; the choke router plus DMZ architecture specifically prevents direct exposure by design and enforces a controlled boundary.

SAMPLE

6. For shared hosting providers, what is required to protect hosted environments?

A. The hosting provider is solely responsible for customer PCI DSS compliance

B. Customers' data in hosted environments is not subject to PCI DSS

C. Shared hosting providers protect only the provider's own environment

D. The hosting provider must protect each entity's hosted environment and data; the customer entity must still comply with PCI DSS

Shared hosting creates a multi-tenant environment, so security responsibilities are shared between the provider and each customer. The hosting provider must implement controls that protect every tenant's hosted environment and data, including proper isolation, access controls, patching, vulnerability management, and monitoring to prevent cross-tenant exposure. At the same time, each customer remains responsible for applying PCI DSS controls to its own cardholder data and processes within that hosted space, and for ensuring their portion of PCI DSS compliance is met. This combination—provider protection of every hosted environment plus ongoing customer compliance for their data—is the correct approach. The other options incorrectly assign sole responsibility to the provider, exempt customer data from PCI DSS, or limit the provider's protections to only their own environment.

7. Which statement correctly describes HTTPS?

A. It uses an insecure plain text channel.

B. It is HTTP over SSL/TLS, providing authentication and encryption for sensitive communications.

C. It is FTP over TLS for secure file transfer only.

D. It is a protocol for secure email transfer.

HTTPS is HTTP run over TLS/SSL, which adds encryption and authentication to web traffic. This means the data between your browser and the server is encrypted, protecting confidentiality; it also safeguards integrity so data can't be tampered with without detection; and it authenticates the server (via a certificate) so you're talking to the legitimate site. This combination is what makes HTTPS suitable for sensitive communications like login credentials and payments. The other descriptions describe different things: an insecure plain text channel would expose data, which HTTPS avoids; FTP over TLS is a separate secure file-transfer protocol (FTPS), not how regular web pages are delivered; and secure email transfer protocols refer to mail, not web traffic.

8. What is the primary objective of PCI DSS Requirement 1?

A. Establish a documented incident response plan.

B. Encrypt all data at rest.

C. Install & maintain a firewall configuration to protect cardholder data.

D. Monitor network activity continuously.

The main idea is to create a secure boundary for the cardholder data environment by controlling network traffic with a firewall. Requirement 1 focuses on installing and maintaining a firewall configuration that sits between untrusted networks (like the Internet) and the networks that handle cardholder data, and enforcing access controls between segments. This means documenting rules, restricting inbound and outbound traffic to only what is necessary, and keeping firewall configurations up to date so unauthorized connections to the cardholder data environment are blocked. Why this is the best fit among the options: it directly addresses building a protective barrier around where cardholder data flows, which is the foundational network security control for PCI DSS. The other options involve incident response planning, encryption of data at rest, and continuous monitoring—important security activities, but they are not the primary objective of firewall configuration.

SAMPLE

9. Which practice is commonly included to mitigate broken authentication and session management?

A. Exposing session IDs in the URL

B. Flagging session tokens as secure

C. Using a fixed, long-lived session ID for convenience

D. Disabling timeouts

Protecting session tokens is essential to preventing session hijacking. Marking the session cookie as Secure ensures it is sent only over HTTPS, so the token isn't exposed in plaintext on insecure connections. This reduces the risk of interception during transmission and helps keep authenticated sessions protected, especially when paired with HttpOnly (to block access from scripts) and SameSite (to mitigate cross-site request forgery). Exposing session IDs in the URL is risky because URLs can be logged in browser history, server logs, and referred by headers, making the token easily discoverable. Using a fixed, long lived session ID means a stolen token could be reused for a long time, increasing impact. Disabling timeouts leaves sessions open indefinitely, allowing ongoing use if a token is compromised. Marking the session token as Secure directly addresses the risk of token theft in transit and aligns with proper session management practices.

10. ISO is described as which type of organization?

A. A governmental organization.

B. A non-governmental organization consisting of national standards institutes.

C. A private corporation.

D. An international regulatory body.

ISO is a non-governmental organization formed by national standards institutes from many countries to develop and publish international standards. It operates independently of any government and does not function as a private corporation or as an international regulatory body. Governments and industries may adopt ISO standards, but ISO itself does not have enforcement power.

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://pcidssrequirements.examzify.com

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

SAMPLE