PCI FUNDAMENTALS PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://pcifundamentals.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. In PCI DSS terms, what is the cardholder environment?

A. The environment used for general business operations with no cardholder data.

B. The environment used exclusively for marketing data.

C. The environment where cardholder data is processed, stored, or transmitted.

D. The environment outside the organization's network where card data is never stored.

2. What is an Attestation of Compliance (AOC)?

A. A formal document signed by the entity stating that PCI DSS controls are implemented and validated, and that the organization is in compliance

B. A vulnerability assessment report

C. A bank accreditation letter

D. An Attestation of Compliance is a formal document signed by the organization stating that PCI DSS controls are implemented and validated, and that the organization is in compliance

3. Which credentialed roles are authorized to perform official PCI DSS assessments?

A. External Security Auditor

B. Compliance Officer

C. Qualified Security Assessor (QSA) or Internal Security Assessor (ISA)

D. IT Technician

4. This is Hardware and/or software used to process payment card transactions at merchant locations:

A. Payment Gateway

B. Network Switch

C. POS/POI

D. Customer Relationship Management

5. What is the purpose of pre-engagement due diligence before engaging a service provider?

A. To select the provider with the lowest cost.

B. To ensure the provider can process more transactions.

C. To ensure the provider has controls to protect cardholder data.

D. To avoid signing a contract.

SAMPLE

6. Which term defines the environment that contains all systems storing, processing, or transmitting cardholder data?

A. Cardholder Data Environment

B. Demilitarized Zone

C. Payment Gateway

D. Tokenization Layer

7. Who is typically responsible for penalties for PCI DSS non-compliance?

A. Payment card brands

B. Merchants

C. Banks

D. Cardholders

8. When must external penetration testing be performed according to PCI DSS?

A. Only after a data breach.

B. Every six months.

C. Only if compliance audits require it.

D. At least annually and after significant changes to the environment.

9. To meet PCI DSS 1.2.1, installing a network firewall between the CDE and corporate network is an example of what security concept?

A. Encryption in transit

B. Segmentation

C. Tokenization

D. Physical separation

10. Which statement describes compensating controls in PCI DSS context?

A. A compensating control replaces the original requirement with a weaker control

B. A compensating control is optional and can be ignored

C. A compensating control provides equivalent or greater protection when a primary requirement cannot be met

D. A compensating control is a type of encryption scheme

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. In PCI DSS terms, what is the cardholder environment?

A. The environment used for general business operations with no cardholder data.

B. The environment used exclusively for marketing data.

C. The environment where cardholder data is processed, stored, or transmitted.

D. The environment outside the organization's network where card data is never stored.

The cardholder environment is the set of systems that handle cardholder data, meaning anything that processes, stores, or transmits that data. This is the scope that PCI DSS focuses on, so all servers, databases, applications, networks, and devices that touch cardholder data fall under protection and controls like encryption, access controls, and monitoring. Environments that only contain non-cardholder data, such as general business or marketing data, are not part of this environment. If card data ever passes through or is stored on a system, that system belongs to the cardholder environment, even if it's within a larger network. In short, the cardholder environment is defined by where cardholder data flows and resides.

2. What is an Attestation of Compliance (AOC)?

A. A formal document signed by the entity stating that PCI DSS controls are implemented and validated, and that the organization is in compliance

B. A vulnerability assessment report

C. A bank accreditation letter

D. An Attestation of Compliance is a formal document signed by the organization stating that PCI DSS controls are implemented and validated, and that the organization is in compliance

An Attestation of Compliance is a formal document signed by the organization that states PCI DSS controls are implemented and validated, and that the organization is in compliance. This document serves as official proof of PCI DSS compliance for payment brands and acquiring banks, often outlining the scope and validation method used. It's the organizational declaration that the controls are in place and functioning as required, typically paired with the supporting assessment (like a ROC or SAQ) but focused on the organization's written acknowledgment of compliance. It's distinct from a vulnerability assessment report, which lists found weaknesses, and it's not a bank accreditation letter.

SAMPLE

3. Which credentialed roles are authorized to perform official PCI DSS assessments?

A. External Security Auditor

B. Compliance Officer

C. Qualified Security Assessor (QSA) or Internal Security Assessor (ISA)

D. IT Technician

The ability to conduct official PCI DSS assessments is limited to two credentialed roles recognized by the PCI Security Standards Council: Qualified Security Assessor and Internal Security Assessor. A Qualified Security Assessor (QSA) is an external professional contracted to perform the formal assessment and produce the official validation, such as the Report on Compliance (ROC). An Internal Security Assessor (ISA) is an internal staff member trained and authorized to carry out the organization's internal assessment and prepare evidence and findings for review. Together, QSAs and ISAs ensure there is both rigorous external validation and structured internal evaluation of PCI DSS compliance. Other roles described don't have the formal PCI DSS accreditation to perform official assessments. An External Security Auditor may review security controls but isn't a PCI SSC-credentialed assessor for PCI DSS. A Compliance Officer oversees compliance programs but isn't a credentialed PCI DSS assessment professional. An IT Technician typically lacks the specialized PCI DSS training and authorization required to conduct official assessments.

4. This is Hardware and/or software used to process payment card transactions at merchant locations:

A. Payment Gateway

B. Network Switch

C. POS/POI

D. Customer Relationship Management

The main idea is identifying the system that handles card payments right at the point of sale. A POS/POI setup is exactly that: hardware and/or software at the merchant location used to capture card data, process the transaction, and connect with the payment processor to authorize and settle payments. It encompasses the card reader, PIN pad, cash register or terminal, and the accompanying software used during a sale. This is the best choice because it represents the on-site apparatus and software that actually processes each card transaction at checkout. A payment gateway, while related, typically acts as the online bridge that authorizes payments or connects a POS to the processor, and is often used for e-commerce or remote transactions rather than the physical checkout system itself. A network switch is networking gear that routes data on a network, not payment processing. Customer Relationship Management focuses on storing and managing customer data and interactions, not handling payment transactions.

SAMPLE

5. What is the purpose of pre-engagement due diligence before engaging a service provider?

A. To select the provider with the lowest cost.

B. To ensure the provider can process more transactions.

C. To ensure the provider has controls to protect cardholder data.

D. To avoid signing a contract.

Assessing a service provider's controls to protect cardholder data before you engage them is about mitigating risk by ensuring they can safeguard sensitive payment data. You're verifying that the provider has solid security measures in place—such as strong access controls, data encryption, ongoing monitoring, and an established incident response process—so that cardholder information remains protected even when it's handled outside your organization. This pre-engagement check helps ensure the provider can meet PCI DSS requirements and fit with your own security and compliance obligations, reducing the chance that bringing them on board will introduce data breaches or expand your PCI scope inadvertently. It's not about choosing the lowest cost, increasing transaction throughput, or avoiding a contract—the focus is on whether the provider has the right controls to protect cardholder data and support your security posture. In practice, you'd look for evidence like PCI DSS attestations, independent audit reports, clear data flow mappings, and details about how they handle access, encryption, logging, and sub-processors to confirm they can meet your security expectations.

6. Which term defines the environment that contains all systems storing, processing, or transmitting cardholder data?

A. Cardholder Data Environment

B. Demilitarized Zone

C. Payment Gateway

D. Tokenization Layer

Cardholder Data Environment defines the environment that contains all systems storing, processing, or transmitting cardholder data. This boundary includes databases, application servers, storage, networks, and backups that actually handle CHD, along with the security controls that protect those systems. Identifying the CDE is essential for PCI DSS because it flags exactly where CHD is present and where strict protections—such as encryption, access controls, monitoring, and segmentation—must be applied. The other terms relate to parts of the architecture but don't define the full CHD-handling environment: a Demilitarized Zone is a network segment exposed to external networks; a Payment Gateway is a service that authorizes payments and may touch CHD but isn't the entire environment that stores, processes, or transmits it; a Tokenization Layer is a method to replace CHD with tokens, reducing risk but not defining the scope of systems that actually store or process CHD.

7. Who is typically responsible for penalties for PCI DSS non-compliance?

A. Payment card brands

B. Merchants

C. Banks

D. Cardholders

Penalties for PCI DSS non-compliance are imposed by the payment card brands (the networks such as Visa, MasterCard, AmEx, etc.). They enforce PCI DSS across their networks and can issue fines, mandate remediation, or even restrict processing privileges when a merchant or service provider fails to meet requirements. The merchant is the party responsible for achieving and maintaining compliance, and fines or costs typically flow through the merchant's acquiring bank, but the authority to levy those penalties comes from the card brands. Cardholders aren't responsible for PCI penalties.

SAMPLE

8. When must external penetration testing be performed according to PCI DSS?

A. Only after a data breach.

B. Every six months.

C. Only if compliance audits require it.

D. At least annually and after significant changes to the environment.

External penetration testing is about verifying that your network perimeter and external-facing components can withstand attacker attempts and that the security controls protecting the cardholder data environment are effective. PCI DSS requires this testing to be done at least once a year and after any significant changes to the network or its components. This combination ensures that new systems, configurations, or connections don't introduce new vulnerabilities that external attackers could exploit. So, you perform external penetration testing annually to catch ongoing risks, and you also test again after substantial changes—such as adding a new network segment, firewall, or external vendor access—to confirm the changes haven't created new weaknesses. Doing it only after a data breach is reactive and misses proactive risk management; six-month timing isn't the minimum requirement; and testing only when audits require it ignores the need to continuously verify external security.

9. To meet PCI DSS 1.2.1, installing a network firewall between the CDE and corporate network is an example of what security concept?

A. Encryption in transit

B. Segmentation

C. Tokenization

D. Physical separation

Network segmentation is being tested. Putting a firewall between the Cardholder Data Environment (CDE) and the rest of the corporate network creates a boundary that logically isolates the sensitive systems. This lets you enforce strict access controls and filter traffic crossing the boundary, which reduces the attack surface and limits PCI DSS scope to the CDE. It's not encryption in transit, which protects data as it moves but doesn't define network boundaries. It's not tokenization, which replaces data with tokens. It's not physical separation, which requires entirely separate hardware or facilities; segmentation achieves isolation through logical boundaries using firewalls and other controls.

10. Which statement describes compensating controls in PCI DSS context?

A. A compensating control replaces the original requirement with a weaker control

B. A compensating control is optional and can be ignored

C. A compensating control provides equivalent or greater protection when a primary requirement cannot be met

D. A compensating control is a type of encryption scheme

In PCI DSS, compensating controls are alternative security measures that you put in place when you genuinely can't meet a specific requirement due to legitimate technical or business constraints. They must provide protection that is equivalent or greater than what the original requirement would have achieved, not be weaker. They're not optional or something you ignore, and they're not simply a different type of control like an encryption scheme. The idea is to preserve the same level of protection for cardholder data by using well-documented, validated, and continuously monitored controls that achieve the same risk reduction as the original requirement. If you adopt a compensating control, it needs thorough justification, formal approval, and periodic reassessment to ensure it remains effective.

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://pcifundamentals.examzify.com

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

SAMPLE