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

Table of Contents

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.

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!

Questions

1. **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

2. **Differentiate vulnerability scanning from penetration testing.**

   A. Scanning is manual and testing is automated.

   B. Scanning examines physical security; testing checks network vulnerabilities.

   C. Vulnerability scanning automatically identifies known weaknesses; penetration testing attempts to exploit weaknesses to validate risk and test controls.

   D. They are exactly the same.

3. **This SAQ should be used for Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) Terminals - No Electronic Cardholder Data Storage.**

   A. SAQ A

   B. SAQ B-IP

   C. SAQ C-VT

   D. SAQ D

4. **Define the Cardholder Data Environment (CDE).**

   A. The network segment responsible for payment processing security.

   B. All devices that store CHD data.

   C. All people, processes, and technology that store, process, or transmit CHD and/or access system components that handle CHD.

   D. The portion of the network that is PCI DSS compliant.

5. **This can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe:**

   A. Card Security Code

   B. PAN

   C. CVV

   D. Track Data

6. When assessing if cardholder data should be stored, which should not be considered?

A. If Payment brand rules allow for the storage of PAN

B. Whether data is encrypted

C. Business need for storage

D. Data minimization requirements

7. When must critical new security patches be installed?

A. Within 24 hours of release.

B. Within one month of release.

C. Within six months of release.

D. Within one year of release.

8. What action should be taken when CHD is no longer needed?

A. Retain CHD in active systems

B. Encrypt and archive indefinitely

C. Forward CHD to a third party for storage

D. Purge or render unreadable CHD when no longer needed

9. In PCI DSS scoping, which entity is most directly responsible for determining merchant levels?

A. The card brands

B. The Acquiring Bank

C. The PCI Security Standards Council

D. The merchant's security team

10. Documents for PCI DSS Self-Assessment does not include:

A. NIST 800-53 guidelines

B. SAQ templates

C. PCI DSS requirements

D. Attestation of Compliance

Answers

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

Explanations

1. 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.

2. Differentiate vulnerability scanning from penetration testing.

A. Scanning is manual and testing is automated.

B. Scanning examines physical security; testing checks network vulnerabilities.

C. Vulnerability scanning automatically identifies known weaknesses; penetration testing attempts to exploit weaknesses to validate risk and test controls.

D. They are exactly the same.

Vulnerability scanning automatically identifies known weaknesses in systems and configurations by using automated tools and databases of known vulnerabilities. It creates a broad inventory of issues such as missing patches, misconfigurations, weak services, and exposed credentials, often delivering a remediation-focused report and risk ratings. This process is typically automated, wide-ranging, and non-intrusive, aimed at surfacing issues for remediation. Penetration testing operates differently by going beyond identification. It involves a skilled tester using techniques to exploit discovered weaknesses to determine whether an attacker could gain unauthorized access, escalate privileges, or cause impact. It provides practical evidence of risk by demonstrating real-world exploitation and the effectiveness of existing controls, usually within a defined scope and timeframe and often requiring manual, targeted effort. So, the key distinction is that scanning finds and reports vulnerabilities, while penetration testing attempts to exploit them to validate risk and test controls.

3. This SAQ should be used for Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) Terminals - No Electronic Cardholder Data Storage.

A. SAQ A

B. SAQ B-IP

C. SAQ C-VT

D. SAQ D

The key idea here is choosing the self-assessment questionnaire that matches how card data flows in your environment. If you're using stand-alone POS terminals that connect to the processor over an IP network and you're not storing cardholder data electronically on your systems, the questionnaire designed for IP-connected, stand-alone POI devices is the right fit. That setup captures card data at the terminal and sends it to the processor, with no data stored on your side, so the controls focus on securing that IP connection, ensuring the terminal is configured securely, and proving that no CHD is stored locally. This fits best because it doesn't require the broader scope that applies when card data is stored or traverses additional systems (like PC-based payment apps) or larger card processing environments. If data were stored or if the environment included other devices or servers, you'd look to the more comprehensive questionnaire for those scenarios.

4. Define the Cardholder Data Environment (CDE).

A. The network segment responsible for payment processing security.

B. All devices that store CHD data.

C. All people, processes, and technology that store, process, or transmit CHD and/or access system components that handle CHD.

D. The portion of the network that is PCI DSS compliant.

The Cardholder Data Environment represents the scope that includes all people, processes, and technologies that store, process, or transmit cardholder data, and anyone who can access system components that handle CHD. This broad definition ensures that every touchpoint with CHD—whether a device, a software process, or a person who interacts with those systems—is covered by PCI DSS controls. The idea is that security controls must apply wherever CHD could be stored, processed, transmitted, or accessed, so that there aren't gaps where data could be exposed. Narrow options that focus only on a single network segment, only on devices that store CHD, or only on PCI DSS-compliant portions fail to capture the full set of people, processes, and technologies involved in handling CHD.

5. This can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe:

A. Card Security Code

B. PAN

C. CVV

D. Track Data

Track data is the data encoded on the magnetic stripe of a card. The stripe is organized into tracks, with track 1 and track 2 carrying different formats, but both containing the essential card information such as the PAN, expiration date, and service code. When we refer to the magnetic-stripe image or the data on track 1 and/or track 2, we're talking about that encoded information—the track data. Card Security Code and CVV are separate verification values, not the data stored on the magnetic stripe, and while the PAN is part of track data, the term that encompasses the whole stripe data is track data.

6. When assessing if cardholder data should be stored, which should not be considered?

A. If Payment brand rules allow for the storage of PAN

B. Whether data is encrypted

C. Business need for storage

D. Data minimization requirements

The decision to store cardholder data should be driven by necessity and security, not by whether a payment brand allows it. You evaluate whether there is a legitimate business need to retain the data (business need) and you apply data minimization—store only what you truly require. If you do store, you must protect the data with strong controls, such as encryption at rest and strict access controls (encryption) and retain only as long as necessary (data minimization). The fact that a payment brand says storage is allowed should not be the main reason to keep PAN data, because brand allowances can change and storing PAN introduces ongoing risk that must be mitigated with the appropriate controls.

7. When must critical new security patches be installed?

A. Within 24 hours of release.

B. Within one month of release.

C. Within six months of release.

D. Within one year of release.

Patching critical vulnerabilities quickly is essential to limit the window of exposure to attackers. For critical security patches, the standard guidance is to install them within one month of their release. This timeframe keeps defenses up to date without waiting too long for testing and validation, which helps prevent known flaws from being exploited in the wild. In practice, you'd validate the patch in a controlled environment, plan a maintenance window, and deploy it once it's confirmed to not disrupt operations. If a patch is highly risky or incompatible with in-scope systems, you document the exception and monitor risk, but the expectation is still to move toward deployment within roughly 30 days. Waiting 6 months or a year leaves systems exposed to known threats, and requiring immediate 24 hours is generally impractical for most environments.

8. What action should be taken when CHD is no longer needed?

A. Retain CHD in active systems

B. Encrypt and archive indefinitely

C. Forward CHD to a third party for storage

D. Purge or render unreadable CHD when no longer needed

The main idea is secure disposal of cardholder data that you no longer need. When CHD isn't required anymore, you should purge or render it unreadable. Purging means removing the data from all systems and backups so it can't be recovered. Rendering unreadable, such as cryptographic erasure or destroying the storage media, ensures that even if copies exist, the data cannot be read or reconstructed. This approach minimizes how long sensitive information is stored, reducing the risk of exposure and helping limit PCI DSS scope. Keeping CHD in active systems or archiving it indefinitely keeps sensitive data accessible and increases risk and maintenance burdens. Moving CHD to a third party for storage adds another party to trust and manage, but it still leaves you responsible for ensuring proper retention limits and secure disposal, and it doesn't eliminate the need to purge when no longer required.

9. In PCI DSS scoping, which entity is most directly responsible for determining merchant levels?

A. The card brands

B. The Acquiring Bank

C. The PCI Security Standards Council

D. The merchant's security team

Merchant levels are used to decide which PCI DSS validation path a merchant must follow based on annual card volume. While card brands publish the thresholds, the acquiring bank—the merchant's payment processor and sponsor with the card brands—actually applies those criteria to the merchant's account, determines the level, and communicates the required validation path (saq vs. roc, and frequency). The PCI Security Standards Council sets the standards themselves, but does not assign merchant levels to individual merchants. The merchant's security team implements the needed controls, but they don't determine the level. So the entity that directly determines merchant levels is the acquiring bank.

10. Documents for PCI DSS Self-Assessment does not include:

A. NIST 800-53 guidelines

B. SAQ templates

C. PCI DSS requirements

D. Attestation of Compliance

NIST 800-53 guidelines are not part of the PCI DSS Self-Assessment documents. The Self-Assessment process centers on the PCI DSS requirements themselves, using SAQ templates to collect responses and an Attestation of Compliance to certify the results. Those three elements—the PCI DSS requirements, the SAQ templates, and the Attestation of Compliance—are the standard pieces in PCI DSS self-assessment. NIST 800-53 guidelines come from a different framework and aren't a required or included component of the PCI DSS Self-Assessment package, though some organizations may reference them for broader security benchmarking.

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!