PCI Data Security Standard Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

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. **Which statement best describes requirement 9.7.1 regarding media inventories?**

   A. Inventory logs of all media must be maintained.

   B. Inventory logs of all media must be maintained and media inventories conducted at least annually.

   C. Inventories must be conducted monthly.

   D. Inventories are optional.

2. **Which statement accurately reflects SSL and early TLS policy after the transition date?**

   A. New implementations must still use SSL or early TLS.

   B. New implementations must not use SSL or early TLS; existing implementations may continue only with a formal migration plan.

   C. SSL/early TLS may be used in new deployments if approved.

   D. POS POI terminals are exempt from SSL/TLS restrictions.

3. **What must organizations maintain when dealing with service providers?**

   A. A list of customers.

   B. A list of service providers.

   C. A formal incident response plan.

   D. Only a privacy policy.

4. **From what source should time settings be obtained for security event logging?**

   A. Local server clock

   B. Industry-accepted time sources

   C. Manual administrator input

   D. Satellite time signals

5. **Which PCI DSS requirement emphasizes documenting security policies and procedures for restricting access to cardholder data?**

   A. Requirement 7.3

   B. Requirement 3.2

   C. Requirement 9.5

   D. Requirement 12.1

6. Before engaging service providers, 12.8.3 requires what?

- **A. A process for engaging service providers that includes due diligence prior to engagement.**
- **B. Engage without any due diligence to save time.**
- **C. Only after a security incident.**
- **D. Document a generic form with no security details.**

7. Which statement best describes the policy for sending PANs using end-user messaging technologies?

- **A. PANs may be sent via unprotected channels if recipients are trusted.**
- **B. PANs can be transmitted via secure channels only.**
- **C. Never send unprotected PANs by end-user messaging technologies.**
- **D. End-user messaging is allowed for PAN sharing if encrypted.**

8. The service provider acknowledgement requirement may be satisfied by:

- **A. Always include the exact wording of PCI DSS Requirement 12.9.**
- **B. Be tailored to the agreement and responsibilities; exact wording is not required.**
- **C. Only be provided verbally.**
- **D. Be signed every month.**

9. Which action should be taken immediately for any terminated users?

- **A. Immediately revoke access for any terminated users.**
- **B. Revoke access only after 90 days.**
- **C. Revoke access during annual audits.**
- **D. Do not revoke access for terminated users.**

10. Where should audit trail files be backed up?

- **A. Centralized log server or media difficult to alter**
- **B. Local backup on same server**
- **C. Public cloud storage**
- **D. Printed copies**

Answers

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

Explanations

1. Which statement best describes requirement 9.7.1 regarding media inventories?

A. Inventory logs of all media must be maintained.

B. Inventory logs of all media must be maintained and media inventories conducted at least annually.

C. Inventories must be conducted monthly.

D. Inventories are optional.

This requirement focuses on knowing where every piece of media that could hold cardholder data is, and making sure you verify it regularly. Keeping an inventory log creates a current list of all media—backup tapes, USB drives, external hard drives, laptops, and other devices that might store CHD—and records who owns each item and where it's stored. Conducting media inventories at least annually adds a verification step: you physically check that the log matches what exists, helping to catch missing, misplaced, or decommissioned media and ensuring proper handling or disposal. The best option combines both elements: maintain the inventory log and perform annual inventories. The other statements don't meet the requirement because merely keeping logs doesn't include a formal verification step, monthly inventories aren't the stated minimum, and saying inventories are optional contradicts the need for accountability and verification.

2. Which statement accurately reflects SSL and early TLS policy after the transition date?

A. New implementations must still use SSL or early TLS.

B. New implementations must not use SSL or early TLS; existing implementations may continue only with a formal migration plan.

C. SSL/early TLS may be used in new deployments if approved.

D. POS POI terminals are exempt from SSL/TLS restrictions.

After the transition date, SSL and early TLS are considered unacceptable for new deployments. The goal is to enforce modern cryptography and close known vulnerabilities in older protocol versions. Therefore, new implementations are prohibited from using SSL or early TLS. If an organization already has SSL/early TLS in use, it may continue only if there is a formal, documented migration plan with clear milestones to remove those protocols and move to TLS 1.2 or higher (ideally TLS 1.2+ or TLS 1.3) within a defined timeline. This combination—no new use and a mandated migration plan for existing deployments—is why the statement is correct. The other options imply exceptions or approvals that PCI DSS does not authorize, and there are no exemptions for any device category like POS terminals.

3. What must organizations maintain when dealing with service providers?

A. A list of customers.

B. A list of service providers.

C. A formal incident response plan.

D. Only a privacy policy.

When dealing with third parties in a PCI context, you need to maintain an up-to-date list of all service providers. This keeps track of every external entity that has access to cardholder data or the systems that support it, along with contact details and what each provider is used for. Having this roster makes it possible to perform ongoing risk assessments, ensure contractual security requirements are in place, and coordinate security reviews and incident responses with the right people at the right time. It also supports timely notifications and accountability if a breach or change occurs. A simple list of customers doesn't address vendor risk or who is handling cardholder data. While a formal incident response plan is important, it's a separate component of the security program and doesn't by itself fulfill the need to catalog service providers. A privacy policy is essential for overall data handling, but it doesn't specifically manage or document your external service relationships.

4. From what source should time settings be obtained for security event logging?

A. Local server clock

B. Industry-accepted time sources

C. Manual administrator input

D. Satellite time signals

Time stamps in security event logs must line up across all systems so you can accurately trace what happened and when. The reliable way to achieve that is to obtain time settings from industry-accepted time sources—typically through network time protocol (NTP) servers that are synchronized to UTC from trusted reference clocks (like GPS or radio time). This provides a single, authoritative time reference that all devices can use, so every log entry shares a common baseline. Relying on a local server clock invites drift, and clocks on different devices drift at different rates, causing mismatched timestamps that break event correlation. Manually inputting time is slow, error-prone, and not scalable—any lapse in updating times across devices can create gaps or misalignment in logs. Satellite time signals can feed a time service, but the robust approach is to rely on centralized, industry-accepted time sources that your network devices consistently query, ensuring accuracy and redundancy across the logging infrastructure.

5. Which PCI DSS requirement emphasizes documenting security policies and procedures for restricting access to cardholder data?

A. Requirement 7.3

B. Requirement 3.2

C. Requirement 9.5

D. Requirement 12.1

The main idea here is that access to cardholder data must be governed by a clearly documented policy. This requirement asks you to establish, publish, and maintain a formal policy that defines who may access CHD, under what conditions, and how those access permissions are granted, reviewed, and revoked. Having this policy documented ensures consistent enforcement of the need-to-know principle and makes accountability and audits straightforward, since everyone follows a published rule set rather than ad hoc decisions. Other controls may address specific technical or procedural aspects, but they don't emphasize the practice of documenting the access-restriction policy itself, which is why this one best matches the prompt.

6. Before engaging service providers, 12.8.3 requires what?

A. A process for engaging service providers that includes due diligence prior to engagement.

B. Engage without any due diligence to save time.

C. Only after a security incident.

D. Document a generic form with no security details.

A formal process for engaging service providers that includes due diligence before engagement. PCI DSS requires you to assess and document a provider's security posture and controls before granting access to cardholder data, and to outline security responsibilities in a written agreement. This pre-engagement due diligence helps prevent data exposure by third parties and sets expectations for ongoing oversight, incident response, data handling, and subcontractor management. Having due diligence up front means you verify that the provider meets security requirements, understand how they handle data, and ensure contracts require specific security controls and responsibilities. This proactive approach reduces risk and aligns with PCI DSS goals of protecting cardholder data. Engaging without due diligence postpones risk assessment, which can lead to gaps and incidents. Waiting until after a security event is too late, and a generic form with no security details fails to establish concrete protections or responsibilities.

7. Which statement best describes the policy for sending PANs using end-user messaging technologies?

A. PANs may be sent via unprotected channels if recipients are trusted.

B. PANs can be transmitted via secure channels only.

C. Never send unprotected PANs by end-user messaging technologies.

D. End-user messaging is allowed for PAN sharing if encrypted.

The policy hinges on not exposing cardholder data through consumer-style messaging channels. End-user messaging technologies—text, chat apps, email, and similar tools—are outside controlled, PCI-compliant environments, and data can be intercepted, stored on devices you don't control, or logged along the way. Because of that risk, the rule is to never send PANs unprotected through these channels. If card data must be shared, use PCI-compliant secure methods (such as tokenization, secure portals, or encrypted transmission within a controlled system) and minimize exposure by redacting PANs to the last four digits when possible. That's why this statement is the best fit: end-user messaging should not be used for transmitting PANs in any unprotected form.

8. The service provider acknowledgement requirement may be satisfied by:

A. Always include the exact wording of PCI DSS Requirement 12.9.

B. Be tailored to the agreement and responsibilities; exact wording is not required.

C. Only be provided verbally.

D. Be signed every month.

Understanding how service provider acknowledgement works is about documenting who is responsible for protecting cardholder data when third parties are involved. The requirement is satisfied by a written agreement or formal process that clearly outlines the service provider's security duties and how they align with the card data environment; you don't need to copy the exact PCI DSS wording into the contract. Tailoring the acknowledgement to the specific services and responsibilities ensures both sides know who does what, how compliance will be demonstrated, and how changes or incidents will be handled. Verbal acknowledgement isn't sufficient because a formal, enforceable record is needed, and signing every month isn't a standard requirement.

9. Which action should be taken immediately for any terminated users?

A. Immediately revoke access for any terminated users.

B. Revoke access only after 90 days.

C. Revoke access during annual audits.

D. Do not revoke access for terminated users.

When a user is terminated, access must be revoked immediately to prevent any chance of the former employee reaching systems or data. This is a core control in PCI DSS: promptly removing the individual's access stops potential misuse and protects cardholder data from being exposed after departure. An immediate offboarding step typically involves disabling or deleting accounts, revoking authentication tokens, and removing the user from privileged groups, across all systems and networks. Delays—such as waiting days, tying revocation to audits, or not revoking at all—create a window where unauthorized access could occur and lead to a breach or noncompliance. So, the safest and correct action is to revoke access right away.

10. Where should audit trail files be backed up?

A. Centralized log server or media difficult to alter

B. Local backup on same server

C. Public cloud storage

D. Printed copies

Auditing and monitoring require that audit trails be preserved intact and retrievable for review. Backing up audit trail files to a centralized log server or to media that is difficult to alter creates a tamper-resistant, centralized repository. This protects evidence of events even if individual systems are compromised, and supports retention and forensic investigations. Centralized storage also allows consistent access controls and easier collection of logs across multiple devices. In contrast, backing up on the same server's local storage risks losing integrity if the server is breached, since both live and backup copies can be altered; public cloud storage might be usable with proper controls but doesn't by itself guarantee immutability unless specific safeguards are in place; printed copies are not practical for large volumes, searchability, or long-term retention.

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://pcidss.examzify.com

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