PCI DSS Requirements 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 vulnerabilities are included in Injection Flaws?

A. SQL injection, LDAP injection, and XPath injection.

B. DNS spoofing and ARP poisoning.

C. Strong authentication and logging.

D. Buffer overflow as the only example.

2. Which account-related activities should be logged to track changes in authentication and privileges?

A. Creation of new accounts, elevation of privileges, and changes to root or admin accounts.

B. Password resets only.

C. Account lockouts only.

D. Logout events only.

3. Which statement about the GSM standard is accurate?

A. It is a standard for mobile devices but is not widely used.

B. It is only used in Europe for voice services.

C. It does not support international roaming between operators.

D. The ubiquity of the GSM standard makes international roaming very common between mobile phone operators.

4. PAN stands for?

A. Primary Account Number

B. Personal Access Number

C. Private Authentication Number

D. Primary Authorization Number

5. What should service providers use when remotely accessing each customer environment?

A. Use The Same Credentials For All Customers

B. Allow Shared Credentials Across Customer Environments

C. Different Authentication Credentials For Access To Each Customer

D. No Credentials Required For Remote Access

6. If manual clear text key mgmt is used, what enforcement is required?

A. Split knowledge and dual control

B. One-person control is sufficient

C. No controls needed

D. Anyone with a password can access

7. Which practice minimizes cardholder data (CHD) storage by enforcing limits on data retention?

A. Specific retention requirements for CHD

B. Limiting data storage amount & retention time to that which is required for legal, regulatory, and/or business requirements

C. A quarterly process for IDing & securely deleting stored CHD that exceeds defined retention

D. Processes for secure deletion of data when no longer needed

8. What does OCTAVE stand for?

A. Open Web Application Security Protocol

B. Organizational Cybersecurity Threat Evaluation

C. Official Certification for Threat Evaluation

D. Operationally Critical Threat, Asset, and Vulnerability Evaluation

9. A smart card is also known as a chip card. What does the chip contain?

A. Only plaintext cardholder data

B. Integrated circuits embedded within; data including data equivalent to magnetic-stripe data

C. Only a PIN

D. No card data; just cryptographic keys

10. What is the minimum retention period for the visitor log, unless restricted by law?

A. Retain this log for six months.

B. Retain the log for at least three months.

C. Retain the log for one year.

D. Retain the log for 30 days.

Answers

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

Explanations

1. Which vulnerabilities are included in Injection Flaws?

A. SQL injection, LDAP injection, and XPath injection.

B. DNS spoofing and ARP poisoning.

C. Strong authentication and logging.

D. Buffer overflow as the only example.

Injection flaws happen when untrusted input is treated as part of a command or query by an interpreter, allowing the attacker to alter the intended logic or execution. SQL injection, LDAP injection, and XPath injection are classic examples because they all involve taking input and embedding it into a query language (SQL, LDAP, or XPath) without proper validation or parameterization. This means that malicious input can modify the query's structure and permissions, potentially exposing data or bypassing authentication. The other options don't describe injection flaws. DNS spoofing and ARP poisoning are network-layer attacks aimed at misleading or intercepting traffic rather than injecting code into a query or command. Strong authentication and logging are security controls and practices, not injection vulnerabilities. Buffer overflow is a memory safety issue where writing past allocated boundaries can crash or hijack a program, which is a different category from injecting untrusted input into a query.

2. Which account-related activities should be logged to track changes in authentication and privileges?

A. Creation of new accounts, elevation of privileges, and changes to root or admin accounts.

B. Password resets only.

C. Account lockouts only.

D. Logout events only.

Tracking changes in authentication and privileges relies on recording account lifecycle events and any adjustments to access rights. Creating a new account introduces a new user with potential access to systems and data, so noting when this happens is essential. Elevation of privileges shows who gains higher levels of access, which can dramatically change what a user can do. Changes to root or admin accounts are especially sensitive because those accounts control critical systems and data; logging those alterations helps detect unauthorized or risky activity and supports forensic investigations. PCI DSS requires automated audit trails that can reconstruct events related to user access and permissions, including who did what, when, and to which resource. The combination of creation of new accounts, privilege elevation, and changes to high-privilege accounts provides a complete picture of authorization changes, enabling effective monitoring and incident response. Password resets are important for authentication but don't necessarily reveal changes in who has access or what level of access they hold. Account lockouts and logout events capture authentication activity but not alterations to account provisioning or privileges. Therefore, the most comprehensive and relevant logging for tracking changes in authentication and privileges is the creation of new accounts, elevation of privileges, and changes to root or admin accounts.

3. Which statement about the GSM standard is accurate?

A. It is a standard for mobile devices but is not widely used.

B. It is only used in Europe for voice services.

C. It does not support international roaming between operators.

D. The ubiquity of the GSM standard makes international roaming very common between mobile phone operators.

GSM's global adoption enables international roaming between networks. GSM, or Global System for Mobile communications, was designed as a common, interoperable standard used by operators around the world. Because many networks share the same standard and use SIM-based authentication, a phone can operate on foreign networks and still access service. This interoperability is what makes roaming across borders so common, since operators establish roaming agreements to allow customers to use voice, text, and data abroad. The other statements don't fit because GSM isn't limited to Europe, isn't restricted from roaming, and isn't accurately described as rarely used. The widespread, international footprint and the roaming framework together explain why roaming is so prevalent.

4. PAN stands for?

A. Primary Account Number

B. Personal Access Number

C. Private Authentication Number

D. Primary Authorization Number

The term PAN refers to the Primary Account Number, which is the unique 15- to 16-digit (up to 19 digits in some cards) number printed on a payment card that identifies the cardholder's account within the issuer's system. This number is the main identifier used during authorization and settlement, linking the transaction to the correct account. In PCI DSS, PAN is treated as cardholder data and must be protected—displayed only in masked form, stored securely, and transmitted with proper cryptographic protections. The other options do not reflect the standard terminology used in payment card processing, so they aren't correct.

5. What should service providers use when remotely accessing each customer environment?

A. Use The Same Credentials For All Customers

B. Allow Shared Credentials Across Customer Environments

C. Different Authentication Credentials For Access To Each Customer

D. No Credentials Required For Remote Access

Requiring different authentication credentials for each customer environment ensures proper isolation, accountability, and control. With unique credentials per customer, access can be granted and revoked on a per-environment basis, and all activity can be traced to the specific customer and user involved. If the same credentials were used across multiple customers or credentials were shared, a compromise could expose many environments at once, making it hard to determine who accessed what and delaying incident response. This approach also supports the PCI DSS need for unique IDs and monitored remote access, often alongside strong authentication, so that privilege and access can be managed precisely per customer. For remote access, using proper credentials (and ideally MFA) rather than no credentials at all is essential to maintain security, auditability, and the integrity of each customer's environment.

6. If manual clear text key mgmt is used, what enforcement is required?

A. Split knowledge and dual control

B. One-person control is sufficient

C. No controls needed

D. Anyone with a password can access

When you manage encryption keys in clear text by hand, you introduce a high risk that a single person could misuse or expose the keys. To counter that risk, the controls require split knowledge and dual control for key management. This means the key's handling is divided among multiple people and sensitive actions to generate, store, rotate, or use the key require at least two individuals to cooperate. No single person should have full access or the ability to perform critical steps alone. This approach minimizes insider threat and reduces the chance of an accidental or deliberate disclosure of cardholder data.

7. Which practice minimizes cardholder data (CHD) storage by enforcing limits on data retention?

A. Specific retention requirements for CHD

B. Limiting data storage amount & retention time to that which is required for legal, regulatory, and/or business requirements

C. A quarterly process for IDing & securely deleting stored CHD that exceeds defined retention

D. Processes for secure deletion of data when no longer needed

Limiting what you store and for how long is the most effective way to reduce cardholder data because it enforces data minimization from the outset. By keeping CHD only as long as legally, regulatorily, or business-reasonably required, you prevent unnecessary data retention and automatically shrink the scope of sensitive information that could be exposed. This proactive approach directly reduces risk and the amount of data that needs protection, monitoring, and later deletion. Other practices—like identifying and securely deleting data that has exceeded a defined retention, or deleting data when it's no longer needed—are important safeguards but are reactive or narrower in scope. They don't guarantee that data isn't stored longer than necessary in the first place. Setting explicit limits on both data quantity and retention time ensures CHD is kept only for the minimal, required period.

8. What does OCTAVE stand for?

A. Open Web Application Security Protocol

B. Organizational Cybersecurity Threat Evaluation

C. Official Certification for Threat Evaluation

D. Operationally Critical Threat, Asset, and Vulnerability Evaluation

OCTAVE is about evaluating information security risk in an organization by focusing on what is critical to operations, the threats those assets face, and the vulnerabilities that could be exploited. The name itself captures this emphasis: Operationally Critical Threat, Asset, and Vulnerability Evaluation. That exact wording shows that the framework centers on operational impact, the assets at risk, the threats to those assets, and the vulnerabilities that could be exploited, guiding how organizations assess and manage risk. The other proposed phrases don't match OCTAVE's established meaning. It isn't Open Web Application Security Protocol, nor Organizational Cybersecurity Threat Evaluation, nor Official Certification for Threat Evaluation. The correct expansion explicitly includes operational context, critical assets, and vulnerabilities, which is why it's the best answer.

9. A smart card is also known as a chip card. What does the chip contain?

A. Only plaintext cardholder data

B. Integrated circuits embedded within; data including data equivalent to magnetic-stripe data

C. Only a PIN

D. No card data; just cryptographic keys

A smart card contains an embedded integrated circuit that provides processing and storage for the card's data and cryptographic keys, and it can emulate magnetic-stripe data to remain compatible with systems that expect track data. This means the chip isn't limited to plain cardholder data or a single PIN; it holds application data, keys, and data that may resemble magnetic-stripe data so older readers can still work. The other descriptions miss the hardware aspect or the range of data stored on the chip: it's not just plaintext data, not only a PIN, and not devoid of data beyond keys.

10. What is the minimum retention period for the visitor log, unless restricted by law?

A. Retain this log for six months.

B. Retain the log for at least three months.

C. Retain the log for one year.

D. Retain the log for 30 days.

Keep the visitor log for at least three months. This baseline provides enough historical data to identify who entered secure areas and when, which supports investigations, audits, and security monitoring. You can retain longer if law or internal policy requires it, but three months is the minimum. Retaining only 30 days is typically too short for effective review, while six months or a year exceed the minimum unless specifically mandated by law or policy.

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!