PCI DATA SECURITY STANDARD PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://pcidss.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. 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

2. 12.3.7 requires?

A. List of company-approved products

B. Acceptable uses of the technology

C. A method to determine owner

D. Explicit approval by authorized parties

3. Penetration testing must review threats and vulnerabilities experienced in the last 12 months.

A. Not Required

B. Last Quarter

C. Last 5 Years

D. Last 12 Months

4. Under 6.5.1, which types of injection flaws are considered?

A. Cross-site scripting only

B. Injection flaws, particularly SQL injection; also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws

C. Buffer overflow only

D. Authentication only

5. In which scenario is background screening considered a recommendation rather than a requirement?

A. Mandatory for all such positions.

B. Not required at all.

C. A recommendation only.

D. Required every six months.

6. What should enforcement of onsite personnel and visitor identification procedures include?

A. Identifying onsite personnel and visitors, noting changes to access requirements, and revoking expired visitor IDs.

B. Identifying only employees, not visitors.

C. Visitor IDs are unnecessary.

D. Identifying visitors only during emergencies.

7. Which practice is recommended when dealing with devices during maintenance?

A. Install or replace devices immediately upon request.

B. Return devices to the vendor without verification.

C. Install, replace, or return devices only after a full-day approval process.

D. Do not install, replace, or return devices without verification.

8. Which diagram must exist to map cardholder data flows across systems and networks?

A. An outdated diagram that only shows external connections.

B. A diagram of security controls without data flow details.

C. A high-level diagram of network topology without data flows.

D. Current diagram that shows all cardholder data flows across systems and networks.

9. As of June 30, 2015, which vulnerability becomes a formal requirement?

A. Insecure cryptographic storage

B. Broken authentication and session management

C. Improper error handling

D. Buffer overflows

10. What is true regarding public-facing web applications and controls?

A. Public-facing web applications require no additional controls.

B. Public-facing web applications must be hosted on isolated networks with no external access.

C. Public-facing web applications are also subject to additional controls to address ongoing threats and ensure secure coding practices.

D. Public-facing web applications bypass secure coding guidelines.

Answers

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

Explanations

1. 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.

2. 12.3.7 requires?

A. List of company-approved products

B. Acceptable uses of the technology

C. A method to determine owner

D. Explicit approval by authorized parties

The essential idea here is about controlling what technologies are allowed to be used in the PCI environment. Having a list of company-approved products creates a formal, auditable catalog of hardware and software that have been evaluated and authorized for use. This catalog helps ensure that only vetted, properly configured items are deployed, making it easier to enforce security standards, track changes, and demonstrate compliance during audits. Why this fits best: a defined approved-products list serves as the concrete artifact that organizations can rely on to enforce governance, reduce the risk of introducing untested or insecure components, and simplify ongoing management like patching and configuration verification. It establishes a baseline for what is permitted and provides a clear reference for both IT and security teams. Why the other ideas aren't as fitting: describing acceptable uses of the technology focuses on user or operational behavior rather than the actual inventory of permitted technologies. A method to determine owner emphasizes ownership responsibility, which is important but does not specify the catalog that enforces what's allowed in the environment. Explicit approval by authorized parties speaks to who signs off on changes, but the requirement is best satisfied by having a tangible list of approved products as the enforceable artifact.

3. Penetration testing must review threats and vulnerabilities experienced in the last 12 months.

A. Not Required

B. Last Quarter

C. Last 5 Years

D. Last 12 Months

Penetration testing needs to reflect the current threat landscape and the vulnerabilities that could realistically affect the environment. Reviewing threats and vulnerabilities experienced in the last 12 months keeps the test aligned with recent attacker techniques, newly disclosed CVEs, and changes in the environment, so the scenarios and exploited weaknesses are relevant to today's risk level. Choosing a window like last quarter would miss many recent developments, while a window of several years includes outdated issues that may no longer be actionable or present. A window of the last 12 months strikes the right balance, ensuring the test evaluates controls against recent and realistic risks.

4. Under 6.5.1, which types of injection flaws are considered?

A. Cross-site scripting only

B. Injection flaws, particularly SQL injection; also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws

C. Buffer overflow only

D. Authentication only

The main idea here is that 6.5.1 addresses injection flaws in code and applications. Injection flaws happen when untrusted input is fed into an interpreter as part of a command or query, allowing attackers to alter performance or behavior. SQL injection is the most well-known example, but the scope also includes other types like OS Command Injection, LDAP injection, XPath injection, and similar injection methods. So the best answer recognizes injection flaws in general and lists SQL injection while also calling out other injection types, matching the standard's broad focus. The other options miss this breadth: cross-site scripting is a different vulnerability class, buffer overflow isn't about injecting into interpreters, and authentication isn't related to injection flaws.

5. In which scenario is background screening considered a recommendation rather than a requirement?

A. Mandatory for all such positions.

B. Not required at all.

C. A recommendation only.

D. Required every six months.

The key idea here is the level of obligation a policy assigns. When background screening is described as a recommendation, it means the organization sees screening as a prudent, risk-reducing practice but does not make it mandatory for every position or scenario. This allows them to tailor decisions based on factors like how sensitive a role is, what data or systems the person can access, and regulatory context. That's why the best choice is the one that states it as a recommendation only. The other scenarios imply a binding obligation or a strict schedule: making screening mandatory for all such positions, not requiring it at all, or requiring it on a fixed cadence like every six months. Each of those would constitute a requirement or a rigid process, not simply a recommended practice.

6. What should enforcement of onsite personnel and visitor identification procedures include?

A. Identifying onsite personnel and visitors, noting changes to access requirements, and revoking expired visitor IDs.

B. Identifying only employees, not visitors.

C. Visitor IDs are unnecessary.

D. Identifying visitors only during emergencies.

Enforcement of onsite personnel and visitor identification procedures ensures that only authorized people are in secure areas and that access rights are kept current. This means you verify both employees and visitors, keep an up-to-date record of who is on site and their level of access, and promptly reflect any changes to access requirements so someone who should have reduced or increased permissions doesn't retain inappropriate access. It also requires revoking expired visitor IDs to prevent reuse of credentials. This is why the best approach is to identify both onsite personnel and visitors, note changes to access requirements, and revoke expired IDs—together these steps maintain accurate, time-bound control over who can enter sensitive areas. The other options fall short because they omit one or more of these essential elements, such as excluding visitors, claiming visitor IDs are unnecessary, or restricting identification to emergencies only.

7. Which practice is recommended when dealing with devices during maintenance?

A. Install or replace devices immediately upon request.

B. Return devices to the vendor without verification.

C. Install, replace, or return devices only after a full-day approval process.

D. Do not install, replace, or return devices without verification.

During maintenance, any installation, replacement, or return of devices must be verified. This verification is a key part of change-control and tamper-resistance: it ensures the device is authorized, authentic, and has not been tampered with, and that proper records and approvals are in place before proceeding. Verifying before making changes protects the cardholder data environment from introducing untrusted hardware, rogue firmware, or tampered components. It also provides traceability—you know exactly what was changed, by whom, and that it complies with security policies. Options that skip verification or impose unnecessary delays undermine security: installing on request without validation can bring in unknown or compromised devices; returning equipment to a vendor without checking it first risks counterfeit or tampered units; waiting a full day for approval slows maintenance without guaranteeing safer outcomes. The right practice is to confirm authorization and integrity before any installation, replacement, or return.

8. Which diagram must exist to map cardholder data flows across systems and networks?

A. An outdated diagram that only shows external connections.

B. A diagram of security controls without data flow details.

C. A high-level diagram of network topology without data flows.

D. Current diagram that shows all cardholder data flows across systems and networks.

Mapping the exact paths cardholder data takes through your environment is essential. A current diagram that shows all cardholder data flows across systems and networks ensures you can see every route where data travels, every system that processes or stores it, and every pointing point where controls must be applied or monitored. This full, up-to-date view supports effective risk assessment, proper segmentation, and the placement of security measures exactly where data moves, not just where you think it might. An outdated diagram that only shows external connections misses internal data paths, so it can leave risks hidden. A diagram of security controls without data flow details doesn't reveal how data travels or which controls protect each path. A high-level diagram of network topology without data flows fails to show the actual routes cardholder data takes, making it impossible to verify proper coverage. Only the current diagram that explicitly shows all cardholder data flows across systems and networks provides the actionable view needed to protect the data end-to-end.

9. As of June 30, 2015, which vulnerability becomes a formal requirement?

A. Insecure cryptographic storage

B. Broken authentication and session management

C. Improper error handling

D. Buffer overflows

The concept being tested is how PCI DSS formalizes protections for cardholder data at rest. As of June 30, 2015, the standard explicitly requires using strong cryptography to protect stored cardholder data and to manage cryptographic keys securely, which makes insecure cryptographic storage a formal requirement. This focus on encryption and key management directly addresses the risk of data being read if storage is compromised. The other issues—broken authentication and session management, improper error handling, and buffer overflows—are important security concerns in general software development, but they are not the specific formal storage-protection requirement that PCI DSS had formalized at that date.

10. What is true regarding public-facing web applications and controls?

A. Public-facing web applications require no additional controls.

B. Public-facing web applications must be hosted on isolated networks with no external access.

C. Public-facing web applications are also subject to additional controls to address ongoing threats and ensure secure coding practices.

D. Public-facing web applications bypass secure coding guidelines.

Public-facing web applications are exposed to the Internet and face ongoing external threats, so they require additional, layered controls implemented throughout the development and operation lifecycle. The best choice reflects that these apps must adhere to secure coding practices and be supported by ongoing defenses—such as secure SDLC processes, code reviews, regular vulnerability testing, strong authentication and session management, input validation, encryption in transit, and protections like a web application firewall. This approach addresses evolving threats and helps prevent common flaws and misconfigurations that public apps are often targeted for. In contrast, simply assuming no extra controls, or insisting they must be isolated from external access, or bypassing secure coding guidelines, would leave public-facing applications vulnerable and does not align with secure PCI practices.

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!