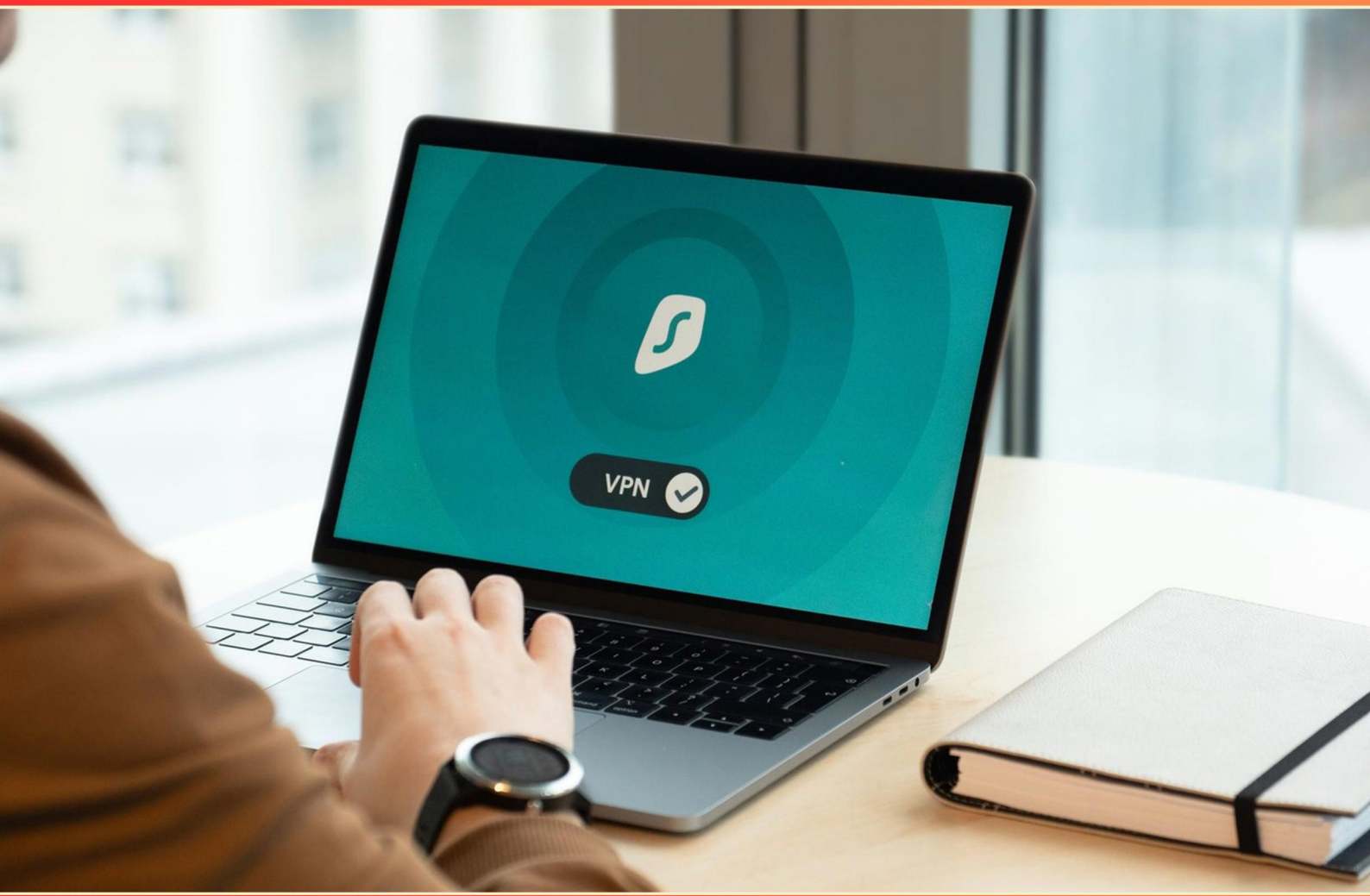
PCI DSS REQUIREMENTS PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://pcidssrequirements.examzify.com

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 16

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 entity is described as the 'merchant bank' in payment card transactions?**

   A. Acquirer

   B. Issuer

   C. Processor

   D. Cardholder

2. **Which practice is commonly included to mitigate broken authentication and session management?**

   A. Exposing session IDs in the URL

   B. Flagging session tokens as secure

   C. Using a fixed, long-lived session ID for convenience

   D. Disabling timeouts

3. **Which statement describes a criterion for compensating controls?**

   A. They meet the intent and rigor of the original PCI DSS requirement

   B. They can rely on existing PCI DSS requirements that are already required for the item under review

   C. They are always cheaper than the original requirement

   D. They do not need to be above and beyond other PCI DSS requirements

4. **Magnetic-Stripe Data is also known as what?**

   A. Card Information

   B. Magnetic Track

   C. Stripe Contents

   D. Track Data

5. **Which statement is NOT a criterion for compensating controls?**

   A. They must meet the intent and rigor of the original PCI DSS requirement

   B. They must provide a similar level of defense

   C. They must be above and beyond other PCI DSS requirements

   D. They do not need to be above and beyond other PCI DSS requirements

6. In addition to annual execution, when else must risk assessments be performed?

A. After every incident

B. Upon significant changes to the environment

C. Never

D. Only during external audits

7. Which statement best describes the status of identification and authentication policies?

A. They Should Be Documented, In Use, And Known To All Affected Parties

B. They Should Be Kept In A Secure Archive

C. They Should Be Updated Annually But Not Distributed

D. They Are Optional For Some Users

8. What does Req 1.1 require to establish and implement?

A. A formal process for approving & testing all network connections & changes to firewall & router configs.

B. A disaster recovery plan.

C. A vulnerability scanning schedule.

D. A data retention policy.

9. What must visitors do with their badge or identification when leaving the facility or when it expires?

A. Surrender the badge or identification before leaving the facility or at expiration.

B. Keep the badge visible at all times while inside the facility.

C. Return the badge only on the next business day.

D. Place the badge in the security bin for later pickup.

10. What is the lifecycle called that includes planning, analysis, design, testing, and implementation?

A. Schema

B. Security Policy

C. Security Event

D. System Development Life Cycle

Answers

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

Explanations

1. Which entity is described as the 'merchant bank' in payment card transactions?

A. Acquirer

B. Issuer

C. Processor

D. Cardholder

In card payment terms, the "merchant bank" is the acquirer. The acquirer is the bank or financial institution that signs a contract with the merchant to enable card acceptance, maintains the merchant account, and handles the flow of funds from cardholders' banks to the merchant. When a payment is made, the acquirer submits the transaction through the card networks to the issuer for authorization, and, once approved, settles the funds to the merchant's account (minus the processor's and network fees). The issuer is the cardholder's bank that issued the card and funds come from that bank if the transaction is approved. The processor is the party that routes the payment data and manages communication between the acquirer, networks, and issuer. The cardholder is the consumer who holds the card.

2. Which practice is commonly included to mitigate broken authentication and session management?

A. Exposing session IDs in the URL

B. Flagging session tokens as secure

C. Using a fixed, long-lived session ID for convenience

D. Disabling timeouts

Protecting session tokens is essential to preventing session hijacking. Marking the session cookie as Secure ensures it is sent only over HTTPS, so the token isn't exposed in plaintext on insecure connections. This reduces the risk of interception during transmission and helps keep authenticated sessions protected, especially when paired with HttpOnly (to block access from scripts) and SameSite (to mitigate cross-site request forgery). Exposing session IDs in the URL is risky because URLs can be logged in browser history, server logs, and referred by headers, making the token easily discoverable. Using a fixed, long lived session ID means a stolen token could be reused for a long time, increasing impact. Disabling timeouts leaves sessions open indefinitely, allowing ongoing use if a token is compromised. Marking the session token as Secure directly addresses the risk of token theft in transit and aligns with proper session management practices.

3. Which statement describes a criterion for compensating controls?

A. They meet the intent and rigor of the original PCI DSS requirement

B. They can rely on existing PCI DSS requirements that are already required for the item under review

C. They are always cheaper than the original requirement

D. They do not need to be above and beyond other PCI DSS requirements

Compensating controls are allowed when you can't meet a PCI DSS requirement as written, but they must deliver protection that is equivalent to the original requirement. The key test is that the compensating controls meet the intent and rigor of the original PCI DSS control, providing at least the same level of protection and being verifiable as such. That's why stating that they meet the original requirement's intent and rigor is the best description. It captures both the purpose (protecting cardholder data in the same way the original control would) and the standard for acceptance (they must be as strong as, or stronger than, the original control and demonstrably achieve its protective goals). Relying on existing PCI DSS requirements alone isn't enough on its own to justify compensating controls, because they must specifically demonstrate equivalent protection to the original requirement. Cost differences don't determine eligibility, since a compensating control can be more or less expensive and still be valid if it preserves the same level of risk mitigation. Finally, the idea that they don't need to be above and beyond other PCI DSS requirements isn't correct; the focus is on achieving equivalent protection, which may involve strengthening controls beyond the bare minimum in some areas to compensate for the gap.

4. Magnetic-Stripe Data is also known as what?

A. Card Information

B. Magnetic Track

C. Stripe Contents

D. Track Data

Magnetic-stripe data refers to the information stored on the card's magnetic stripe, which is read as Track 1 and Track 2 data. In PCI DSS and common card-technology terminology, this data is called Track Data. That's why the option "Track Data" is the best fit. The other terms aren't standard. "Card Information" is too generic, "Magnetic Track" isn't the common label used, and "Stripe Contents" isn't the usual term for the data stored on the stripes.

5. Which statement is NOT a criterion for compensating controls?

A. They must meet the intent and rigor of the original PCI DSS requirement

B. They must provide a similar level of defense

C. They must be above and beyond other PCI DSS requirements

D. They do not need to be above and beyond other PCI DSS requirements

When you can't meet a PCI DSS requirement, compensating controls are alternative measures that must achieve the same level of protection as the original control. They work by preserving the security goal of the requirement even though the exact control wasn't feasible. They must reflect the intent and rigor of the original requirement, meaning they should address the same risk with an approach that matches how strong the original control would have been. They also have to provide a similar level of defense, not a weaker substitute, so the overall protection remains equivalent. Additionally, compensating controls should add protection beyond other PCI DSS requirements, rather than simply reusing existing controls. This extra strength is what makes them an acceptable substitute when the normal control can't be implemented. Therefore, the statement claiming they do not need to be above and beyond other PCI DSS requirements is not a criterion for compensating controls.

6. In addition to annual execution, when else must risk assessments be performed?

A. After every incident

B. Upon significant changes to the environment

C. Never

D. Only during external audits

The main idea is that risk assessments in PCI DSS aren't a one-off annual task; they must be revisited whenever the environment changes in ways that could affect risk. The best choice is to perform a risk assessment upon significant changes to the environment because such changes can introduce new threats, alter how cardholder data flows, or affect the effectiveness of existing controls. Reassessing ensures the risk posture and the controls stay aligned with the current situation. For example, adding a new payment channel, moving data to a cloud service, changing network topology, or onboarding a new third-party processor are all significant changes that can shift risk levels and require updated risk treatment. Choosing to assess risk only after incidents, never, or only during external audits doesn't fit because risk management is ongoing and should respond to changes in the environment, not be limited to incidents or audits.

7. Which statement best describes the status of identification and authentication policies?

A. They Should Be Documented, In Use, And Known To All Affected Parties

B. They Should Be Kept In A Secure Archive

C. They Should Be Updated Annually But Not Distributed

D. They Are Optional For Some Users

The main idea here is that identification and authentication policies must be formal, current, and shared with the people who are affected. Having the policy documented provides a clear standard that can be referenced during audits and daily operations. Keeping the policy in use shows it isn't just a paper exercise; it's part of how access decisions are made. And ensuring that all affected parties know the policy guarantees that everyone understands how to identify and authenticate appropriately, what is allowed, and what isn't. In the PCI DSS context, policies of this kind are required to be documented, implemented, and communicated to personnel so they are aware of the rules governing access. This combination—documented, in use, and known by those who must follow it—helps enforce consistent, secure behavior across the organization. Keeping the policy only in a secure archive misses the enforcement and awareness pieces. Updating annually but not distributing means people may not know the latest rules. Calling it optional for some users undermines the entire access-control framework and creates gaps in security.

8. What does Req 1.1 require to establish and implement?

A. A formal process for approving & testing all network connections & changes to firewall & router configs.

B. A disaster recovery plan.

C. A vulnerability scanning schedule.

D. A data retention policy.

Establishing a formal change-management process for network connections and firewall/router configurations is what this requirement focuses on. The idea is to have a defined, auditable workflow where every change to network connectivity or security devices is reviewed, approved by the right people, and tested in a controlled environment before it goes into production. This helps prevent unapproved or poorly tested changes from creating new security gaps, misconfigurations, or opportunities for data exposure. By documenting approvals, testing results, and the implementation steps, you maintain accountability and traceability for all network-related alterations, which is essential for maintaining a secure cardholder data environment. Disaster recovery planning, vulnerability scanning schedules, and data retention policies address different areas of security and governance. A disaster recovery plan focuses on restoring operations after disruption, vulnerability scanning schedules target identifying weaknesses, and data retention policies govern how long data is kept. None of these ensure the formal approval and testing process for network and security device changes that this requirement mandates.

9. What must visitors do with their badge or identification when leaving the facility or when it expires?

A. Surrender the badge or identification before leaving the facility or at expiration.

B. Keep the badge visible at all times while inside the facility.

C. Return the badge only on the next business day.

D. Place the badge in the security bin for later pickup.

Controlling physical access requires promptly revoking credentials when they're no longer valid. When a visitor leaves the facility or their badge expires, surrendering the badge ensures the access control system can deactivate that credential immediately and update the visitor log. This prevents the badge from being reused to gain entry, keeps records accurate, and reduces the risk of unauthorized access to sensitive areas, such as the cardholder data environment. Keeping the badge visible inside the facility, returning it later, or placing it in a bin for pickup could allow continued or unauthorized access and leaving expired credentials active.

10. What is the lifecycle called that includes planning, analysis, design, testing, and implementation?

A. Schema

B. Security Policy

C. Security Event

D. System Development Life Cycle

The System Development Life Cycle is the organized process for creating or updating information systems, guiding work from planning and requirements gathering through analysis, design, testing, and eventual implementation. This lifecycle provides a structured path to ensure the solution meets needs, is thoroughly tested, and is deployed in a controlled way, with ongoing operation and maintenance afterward. The other terms refer to different concepts: a schema is the structure of a database, a security policy outlines rules for protecting information, and a security event is an observable security-related occurrence. None describe the full, end-to-end process of building or changing a system, so the System Development Life Cycle is the appropriate term.

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!