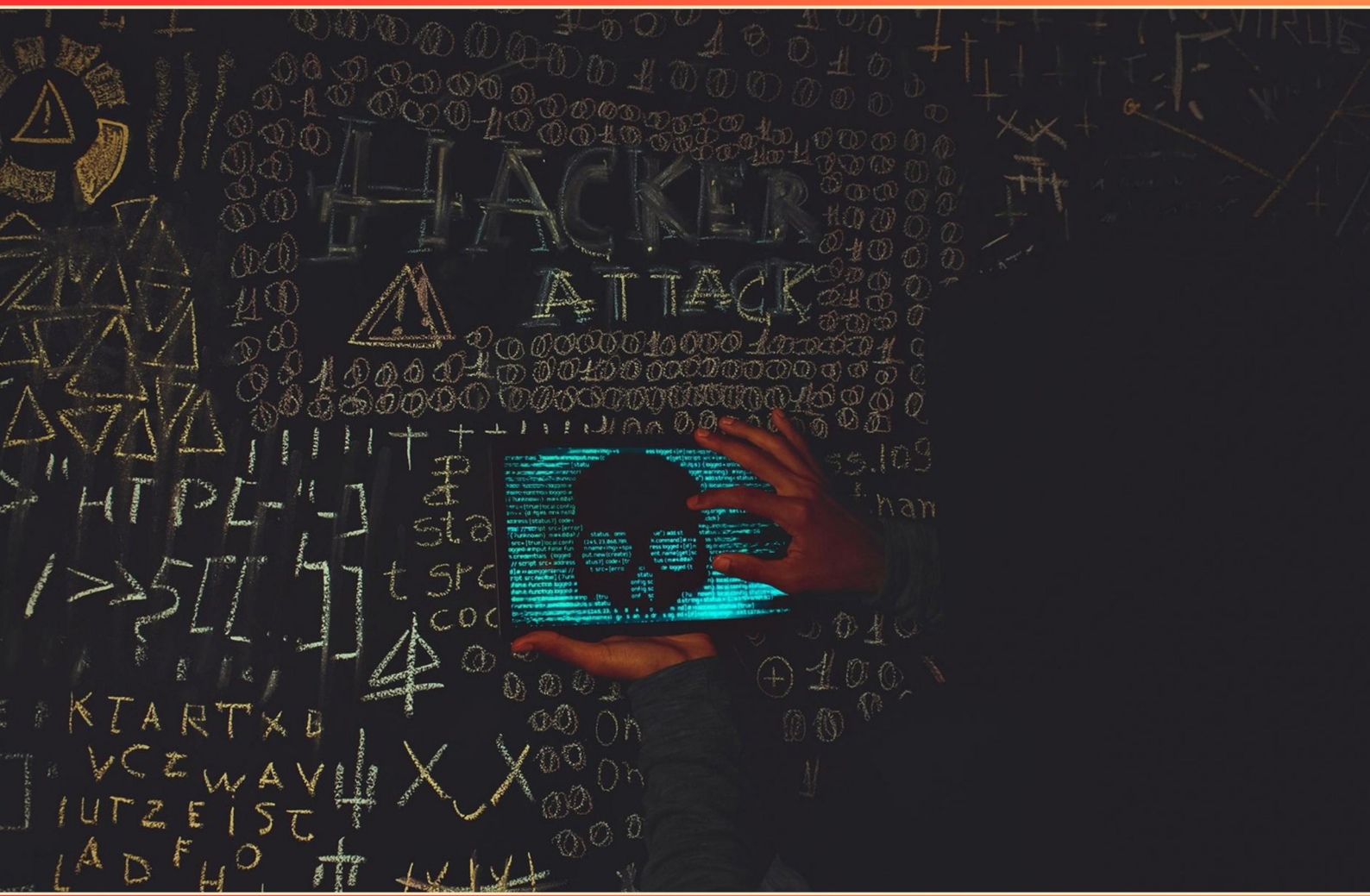
PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://pci-datasecuritystandards.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

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

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. **Which method must assessors use to verify user password changes as required by PCI DSS?**

   A. Set the system clock ahead 90 days to see if password expire

   B. Require a user to change their password, and return in 60 days to see if it has expired

   C. Review system configuration settings to verify passwords must be changed after 90 days

   D. Interview service desk personnel to verify that user passwords are disabled every 60 days

2. **What does the acronym PAN refer to in PCI DSS?**

   A. Primary Account Number

   B. Personal Account Number

   C. Payment Authorization Number

   D. Payment Account Number

3. **How often should a PCI DSS assessment be conducted?**

   A. Monthly

   B. Quarterly

   C. Annually

   D. Bi-annually

4. **According to Requirement 8, what is the minimum complexity requirement for user passwords?**

   A. 5 characters, either alphabetic or numeric

   B. 7 characters, both alphabetic and numeric characters

   C. 6 characters, both alphabetic and numeric characters

   D. 8 characters, either alphabetic or numeric

5. **What is an example of cardholder data that must be protected under PCI DSS?**

   A. The expiration date of a credit card

   B. The card verification value (CVV)

   C. The overall transaction volume of a merchant

   D. The type of payment method used by customers

SAMPLE

6. Which of the following is correct regarding network segmentation?

A. Network segmentation is not a PCI DSS requirement

B. A properly segmented network increases the scope of a PCI DSS assessment

C. A segmented network is also known as a "flat network"

D. Network segmentation is required by PCI DSS for all in-scope networks

7. What should organizations implement to continuously enhance security safeguards?

A. A fixed security protocol

B. Limited training sessions

C. A continual improvement process, including training, updates, and audits

D. Outsourcing security measures to third parties

8. What is the consequence of failing a PCI DSS assessment?

A. The organization will be exempt from compliance measures

B. The organization may face remedial actions, increased scrutiny, and potential financial penalties

C. All employees will receive additional training

D. The organization will receive a grace period to correct issues

9. What is the goal of performing quarterly internal vulnerability scans and rescans?

A. To address all "high-risk" vulnerabilities as defined in PCI DSS requirement 6.1

B. To address all vulnerabilities ranked "low", "medium" or "high" as defined by the ASV

C. To address any vulnerabilities with a CVSS score of 4.0 or lower

D. To address any vulnerabilities with a CVSS score of 7.0 or higher

10. What is the significance of access control in PCI DSS?

A. It allows all employees access to all data

B. It restricts access to cardholder data to only necessary individuals

C. It eliminates the need for encryption in data storage

D. It facilitates unmonitored access to systems

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which method must assessors use to verify user password changes as required by PCI DSS?

A. Set the system clock ahead 90 days to see if password expire

B. Require a user to change their password, and return in 60 days to see if it has expired

C. Review system configuration settings to verify passwords must be changed after 90 days

D. Interview service desk personnel to verify that user passwords are disabled every 60 days

The correct answer involves reviewing system configuration settings to ensure that password changes must occur after a specified period, such as 90 days. This verification process is critical for maintaining the integrity and security of user accounts. By checking the system configuration, assessors can confirm that the organization has established and enforced policies regarding password expiration which are mandated by the PCI Data Security Standards. This approach ensures that users regularly update their passwords, thereby reducing the risk of unauthorized access stemming from forgotten or compromised credentials. Configurations that lead to automatic password expiration are a proactive measure in safeguarding sensitive information within the payment card environment. Reviewing system configurations also provides a clear and documented way to verify compliance without needing to rely on potentially time-consuming testing methods or the subjective accounts from personnel, which could introduce variability in the assessment. This method promotes a structured and auditable approach to compliance verification, aligning with the overarching goals of PCI DSS to protect cardholder data.

2. What does the acronym PAN refer to in PCI DSS?

A. Primary Account Number

B. Personal Account Number

C. Payment Authorization Number

D. Payment Account Number

The acronym PAN stands for Primary Account Number within the context of the Payment Card Industry Data Security Standards (PCI DSS). The Primary Account Number is the unique identifier associated with a cardholder's account that is used for transactions. It typically appears on the front of a credit or debit card and is crucial for processing payments, as it identifies the issuer and the individual account. Correctly identifying this term is vital as understanding the PAN's significance helps organizations implement appropriate security measures to protect cardholder information under PCI DSS. This includes ensuring that systems that store, process, or transmit cardholder data are compliant with required standards to prevent data breaches and unauthorized access to sensitive payment information. Recognizing the correct terminology is also essential for clear communication within the industry regarding payment security and compliance practices.

SAMPLE

3. How often should a PCI DSS assessment be conducted?

A. Monthly

B. Quarterly

C. Annually

D. Bi-annually

The correct choice reflects the requirement established by the PCI Data Security Standards, which mandates that a formal PCI DSS assessment be performed at least annually for organizations that handle or process payment card information. This annual assessment ensures that organizations are continually compliant with the standards and that they maintain the necessary security measures to protect cardholder data. Conducting an assessment annually provides a systematic approach to evaluating and improving security posture. It allows organizations to identify and rectify any vulnerabilities in their systems, as well as to adapt to any changes in technology or business processes that may increase security risks. Additionally, an annual assessment is often sufficient for organizations that have stable systems and practices, allowing them to focus their resources effectively while still fulfilling compliance requirements. While the need for more frequent assessments, such as quarterly or monthly, can arise in response to significant changes in the environment, processing methods, or after data breaches, under normal circumstances, an annual assessment is deemed adequate for maintaining PCI compliance.

4. According to Requirement 8, what is the minimum complexity requirement for user passwords?

A. 5 characters, either alphabetic or numeric

B. 7 characters, both alphabetic and numeric characters

C. 6 characters, both alphabetic and numeric characters

D. 8 characters, either alphabetic or numeric

The correct answer indicates that the minimum complexity requirement for user passwords, as stated in Requirement 8 of the PCI Data Security Standards, is that passwords should be at least 7 characters long and must include both alphabetic and numeric characters. This requirement is in place to enhance security and reduce the vulnerability of user accounts to brute force attacks or other unauthorized access attempts. Requiring a minimum length of 7 characters ensures there is sufficient complexity within the password, making it notably harder for attackers to guess. The incorporation of both alphabetic and numeric characters further strengthens the password by increasing the potential character set used, thereby enhancing the overall randomness and unpredictability of the password. The other options do not meet the specified minimum complexity for passwords, either due to insufficient length or lack of character variety, making them less secure than what is mandated by the PCI standards. This principle of password complexity is crucial for maintaining a strong security posture within organizations that handle payment card information, helping to protect cardholder data and mitigate the risk of breaches.

SAMPLE

5. What is an example of cardholder data that must be protected under PCI DSS?

A. The expiration date of a credit card

B. The card verification value (CVV)

C. The overall transaction volume of a merchant

D. The type of payment method used by customers

The card verification value (CVV) is a crucial piece of information that must be protected under the Payment Card Industry Data Security Standards (PCI DSS). The CVV is a security feature found on credit and debit cards, usually a three or four-digit number that helps verify that the person making a transaction is in possession of the card. This code is not stored with the cardholder's account information after a transaction is completed, as its purpose is to add an extra layer of security against fraud. Given its sensitive nature, protecting the CVV is essential to maintaining the integrity and security of cardholder information. In contrast, while the expiration date of a credit card is considered sensitive information, it is not categorized as cardholder data that needs the same level of protection as the CVV under PCI DSS. Similarly, the overall transaction volume of a merchant and the type of payment method used by customers do not fall into the category of cardholder data and do not require the same security measures as personal identification numbers and codes that could directly facilitate fraud if compromised.

6. Which of the following is correct regarding network segmentation?

A. Network segmentation is not a PCI DSS requirement

B. A properly segmented network increases the scope of a PCI DSS assessment

C. A segmented network is also known as a "flat network"

D. Network segmentation is required by PCI DSS for all in-scope networks

The correct choice highlights a key aspect of PCI DSS requirements: network segmentation itself is not explicitly mandated by the standards, though it is highly recommended. Network segmentation is a practice that can help an organization limit the scope of their PCI DSS assessment by isolating the payment card data environment (PCDE) from other parts of the network. By doing so, only the segmented part containing sensitive payment information would need to comply with strict PCI DSS requirements, thereby reducing the complexity and volume of the assessment process. The other options misinterpret the principles of network segmentation in relation to PCI DSS. While segmentation can help in reducing the scope of PCI compliance assessments, saying it increases the scope is misleading. A segmented network is not classified as a "flat network," which is typically used to describe a network without segmentation. Lastly, while it's beneficial for organizations to adopt network segmentation as a security measure, it's not universally required for all in-scope networks under PCI DSS. Understanding this distinction is crucial for organizations looking to implement effective security measures while maintaining compliance with PCI DSS standards.

SAMPLE

7. What should organizations implement to continuously enhance security safeguards?

A. A fixed security protocol

B. Limited training sessions

C. A continual improvement process, including training, updates, and audits

D. Outsourcing security measures to third parties

Implementing a continual improvement process is essential for organizations seeking to enhance their security safeguards. This approach involves regularly assessing and updating security measures to effectively address emerging threats and vulnerabilities. By incorporating training, updates, and audits into the security framework, organizations can ensure that their team remains informed about the latest security best practices and compliance requirements. Continuous training helps employees recognize and respond to security challenges, while regular updates to security protocols keep the organization ahead of potential risks. Audits provide an opportunity for identifying weaknesses in the security framework and making necessary adjustments. Together, these elements create a dynamic security posture that evolves with the changing landscape of threats, ultimately enhancing overall security and compliance. In contrast, a fixed security protocol lacks the flexibility needed to adapt to new challenges and could leave an organization vulnerable. Limited training sessions do not provide ongoing education and would likely result in employees not being up-to-date with the latest security practices. Outsourcing security measures to third parties can be a part of a strategy but does not guarantee continuous enhancement unless there is a robust partnership in place that includes sharing knowledge and practices for improvement. Thus, the continual improvement process stands out as the most effective means for organizations to advance their security measures consistently.

8. What is the consequence of failing a PCI DSS assessment?

A. The organization will be exempt from compliance measures

B. The organization may face remedial actions, increased scrutiny, and potential financial penalties

C. All employees will receive additional training

D. The organization will receive a grace period to correct issues

Failing a PCI DSS assessment can lead to serious consequences for an organization, including remedial actions, increased scrutiny, and potential financial penalties. This is because PCI DSS compliance is crucial for protecting cardholder data and maintaining trust with customers and payment processors. When an organization fails an assessment, it indicates that there are significant vulnerabilities or lapses in their data protection measures. Consequently, they may be required to implement a plan of action to address these deficiencies. This can involve enhancing security controls, adopting new technologies, or undergoing additional audits to ensure compliance. Financial penalties may arise as a result of non-compliance, particularly if a data breach occurs, leading to legal liability and damage to the organization's reputation. The other options do not accurately reflect the realities of failing a PCI DSS assessment. An organization cannot be exempt from compliance measures following a failure, nor is there an automatic provision for additional training for all employees. While organizations may be given time to rectify issues, this is not easily interpreted as a grace period without demonstrating significant risk mitigation efforts beforehand. Thus, the consequence of failing an assessment includes a series of challenges that organizations must navigate to regain compliance and safeguard their operations.

SAMPLE

9. What is the goal of performing quarterly internal vulnerability scans and rescans?

A. To address all "high-risk" vulnerabilities as defined in PCI DSS requirement 6.1

B. To address all vulnerabilities ranked "low", "medium" or "high" as defined by the ASV

C. To address any vulnerabilities with a CVSS score of 4.0 or lower

D. To address any vulnerabilities with a CVSS score of 7.0 or higher

The goal of performing quarterly internal vulnerability scans and rescans is to identify and address "high-risk" vulnerabilities as defined in PCI DSS requirement 6.1. This requirement emphasizes the importance of proactively managing vulnerabilities within a system to reduce the risk of potential exploitation, which could lead to data breaches or other security incidents. By specifically targeting high-risk vulnerabilities, organizations can prioritize their remediation efforts effectively. This strategic focus ensures that the most critical security gaps are addressed promptly, thus improving the overall security posture of the environment. The rationale behind this is that high-risk vulnerabilities are often the most likely to be exploited by attackers, which can pose significant threats to cardholder data and other sensitive information. Other choices reflect different scopes of vulnerability management that go beyond the immediate focus of PCI DSS requirement 6.1. While addressing low or medium vulnerabilities, or those with varying CVSS scores, can be important for a comprehensive security strategy, the specific context of PCI compliance highlights the necessity to focus efforts on addressing high-risk vulnerabilities as a priority. This aligns with the overarching goals of the PCI DSS to protect payment card information and maintain the integrity of the payment ecosystem.

10. What is the significance of access control in PCI DSS?

A. It allows all employees access to all data

B. It restricts access to cardholder data to only necessary individuals

C. It eliminates the need for encryption in data storage

D. It facilitates unmonitored access to systems

The significance of access control in PCI DSS primarily lies in its role of restricting access to cardholder data to only those individuals whose job responsibilities require such access. This principle of least privilege is crucial in protecting sensitive data and minimizing the risk of data breaches. By ensuring that only authorized personnel can access cardholder information, organizations can better safeguard against unauthorized access and potential data theft. Access control helps in maintaining compliance with PCI DSS requirements, which mandate that entities must implement strong access control measures to protect cardholder data. In doing so, organizations can reduce the potential attack surface and enhance their overall security posture. Effective access control mechanisms include user authentication, role-based access permissions, and regular review of access logs to monitor and manage who has access to sensitive information at all times.

SAMPLE

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://pci-datasecuritystandards.examzify.com

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

SAMPLE