# PCI APPROVED SCANNING VENDOR (ASV) ONLINE PRACTICE TEST (SAMPLE)

## STUDY GUIDE



## SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE**

https://pciasvonline.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 ..... 15


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 two characteristics must passwords meet according to 8.2.1?**

A. Minimum length of 7 characters

B. Must contain numeric and alphabetic characters

C. Both of the above

D. Must include uppercase and lowercase only

**2. Which mitigation technique is commonly used to defend against cross-site scripting (XSS)?**

A. Input validation and output encoding

B. Relying on client-side scripting

C. Storing passwords in plaintext

D. Disable all JavaScript on clients

**3. Which ASV Scan characteristic accounts for load balancers?**

A. Be Accurate

B. Be Platform Independent

C. Perform Service/OS Discovery

D. Account for Load Balancers

**4. Can SSL and Early TLS be used to satisfy PCI DSS requirements?**

A. True

B. False

C. Only when PCI audits are waived

D. Only for non-critical systems

**5. In the Overall Scan Results, what information is not included?**

A. IP addresses

B. Pass/fail status

C. Date for scan expiration

D. Number of components scanned

SAMPLE

**6. A vulnerability which exclusively results in denial-of-service, even if it is over the 4.0 score threshold, is not considered a failing vulnerability.**

A. False

B. Not applicable to PCI

C. True

D. Only with CVSS 7.0

**7. Which statement best describes the difference between best-practice and compliance?**

A. Best-practice may exceed what is sufficient to meet compliance

B. Best-practice is the same as compliance

C. Best-practice is always stricter than compliance

D. There is no difference

**8. What term is key when discussing SSL/TLS suitability for PCI scanning?**

A. Server

B. Host device

C. Client

D. Network

**9. It is compulsory to submit scan report results according to each payment brand's compliance reporting requirements.**

A. SOMETIMES

B. CANNOT BE DETERMINED

C. TRUE

D. FALSE

**10. QIR stands for what?**

A. Qualified Internal Reviewer

B. Qualified Incident Responder

C. Qualified Information Resource

D. Qualified Integrator Reseller

SAMPLE

# Answers

SAMPLE

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

SAMPLE

# Explanations

SAMPLE

## 1. Which two characteristics must passwords meet according to 8.2.1?

A. Minimum length of 7 characters

B. Must contain numeric and alphabetic characters

C. Both of the above

D. Must include uppercase and lowercase only

*Passwords must be long enough and include a mix of character types to resist guessing. For 8.2.1, this means a minimum length of seven characters and the inclusion of numeric characters along with alphabetic characters. The longer length expands the password space, making brute-force attempts far harder, while adding numbers increases complexity beyond purely alphabetical passwords. Together, these two requirements create a stronger baseline than either one alone. If a password only met the length requirement but used only letters, it would still be susceptible to dictionary or pattern-based attacks. If a password met the character-mix requirement but was shorter than seven, it wouldn't provide sufficient protection against guessing. A rule that demands uppercase and lowercase only would omit numeric complexity and, depending on length, might still be weaker than the combined approach.*

## 2. Which mitigation technique is commonly used to defend against cross-site scripting (XSS)?

A. Input validation and output encoding

B. Relying on client-side scripting

C. Storing passwords in plaintext

D. Disable all JavaScript on clients

*Cross-site scripting is prevented by controlling untrusted input and how it's rendered in a browser. The most effective and commonly used defense is to validate inputs to reject dangerous content and to encode data on output so anything potentially harmful is treated as text rather than executable code. Input validation reduces the amount of unsafe data that can enter the system, while output encoding neutralizes data when it's displayed by transforming characters like <, >, &, and quotes into safe HTML entities. The right encoding depends on the context—HTML content needs HTML entity encoding, URLs need URL encoding, and data injected into scripts or attributes requires context-appropriate escaping. Together with broader safeguards like content security policies and proper data sanitization, this approach provides solid protection against XSS. Relying on client-side scripting alone isn't enough because security controls must be enforced on the server and validated by the browser; storing passwords in plaintext has nothing to do with preventing XSS and creates other serious risks; disabling JavaScript on clients is impractical and would break legitimate functionality while not reliably stopping XSS.*

## 3. Which ASV Scan characteristic accounts for load balancers?

A. Be Accurate

B. Be Platform Independent

C. Perform Service/OS Discovery

D. Account for Load Balancers

*Load balancers change what the scanner sees on the network. They can front many backend servers or terminate TLS, presenting a single endpoint to the outside while the actual services run behind it. If you don't account for this, you might miss vulnerabilities on the real backend hosts or misinterpret what the front-end appears to be securing. The ability to account for load balancers ensures the scan covers all underlying hosts and handles front-end behavior like TLS offloading, so the assessment reflects the true security posture behind the load balancer. The other options are broader or unrelated to this specific scenario: accuracy is important in general, platform independence isn't about load balancers, and service/OS discovery focuses on identifying services rather than addressing how traffic is distributed or terminated by a load balancer.*

SAMPLE

## 4. Can SSL and Early TLS be used to satisfy PCI DSS requirements?

A. True

B. False

C. Only when PCI audits are waived

D. Only for non-critical systems

*SSL and early TLS are outdated and insecure for protecting cardholder data in transit. PCI DSS requires strong cryptography and secure protocols, typically TLS 1.2 or higher with current cipher suites. Because SSL and early TLS do not meet these requirements and are explicitly deprecated in PCI guidance, they cannot be used to satisfy PCI DSS. There's no scenario—audits waived or otherwise—where these protocols would be acceptable for systems that handle payment data. Up-to-date TLS is the correct approach.*

## 5. In the Overall Scan Results, what information is not included?

A. IP addresses

B. Pass/fail status

C. Date for scan expiration

D. Number of components scanned

*In an Overall Scan Results view, you get a quick, high-level snapshot of the scan: whether the scan passed or failed, when the current scan results expire (so you know when to rescan for compliance), and how many components were included in the assessment. The specific IP addresses of the scanned hosts aren't shown in this summary; you'd see those details in the per-host or detailed results if you need them. This keeps the overview focused on outcome, timing, and scope, which is what you need to gauge compliance quickly. So, the information not included in the Overall Scan Results is the IP addresses.*

## 6. A vulnerability which exclusively results in denial-of-service, even if it is over the 4.0 score threshold, is not considered a failing vulnerability.

A. False

B. Not applicable to PCI

C. True

D. Only with CVSS 7.0

*Denial-of-service issues that affect only availability do not give an attacker access to cardholder data or the ability to alter it, nor do they directly enable unauthorized system control. PCI ASV guidance focuses on vulnerabilities that could impact the confidentiality, integrity, or secure access of cardholder data. If a vulnerability's impact is exclusively on availability (a DoS), it does not count as a failing vulnerability for PCI DSS purposes, even if its CVSS score is above the 4.0 threshold. The important idea is that the risk from a DoS-only flaw isn't about data exposure or manipulation, so it isn't treated the same as vulnerabilities that could compromise cardholder data. Therefore, the statement is true. The other options don't fit: it isn't False because the DoS-only case isn't treated as failing; it isn't Not applicable to PCI because PCI does consider vulnerability categories and their impact on cardholder data, and it isn't dependent on a specific CVSS version like "Only with CVSS 7.0."*

SAMPLE

## 7. Which statement best describes the difference between best-practice and compliance?

A. Best-practice may exceed what is sufficient to meet compliance

B. Best-practice is the same as compliance

C. Best-practice is always stricter than compliance

D. There is no difference

*The main idea here is that compliance sets the minimum you must meet, while best-practice goes beyond to reduce risk more than those minimum requirements. In PCI DSS terms, being compliant means you implement the controls defined by the standard to pass the assessment. But security professionals often adopt best-practice measures that exceed those minimums, such as adding extra layers of defense, more frequent monitoring, or stricter configurations, to further lower the chance of a breach. So the statement that best-practice may exceed what is sufficient to meet compliance is the best description. For example, PCI DSS might require certain access controls, but best-practice could push you to enforce multi-factor authentication everywhere, implement continuous monitoring, or apply more aggressive patch management. Those extra steps go beyond the bare minimum, which is why best-practice isn't simply the same as compliance and isn't always strictly "more strict" in every single case.*

## 8. What term is key when discussing SSL/TLS suitability for PCI scanning?

A. Server

B. Host device

C. Client

D. Network

*In SSL/TLS suitability checks for PCI scanning, the focus is on the endpoint where the TLS service actually runs and terminates connections—the host device. This is the device that serves certificates, negotiates TLS versions, and selects cipher suites for external clients. PCI DSS looks at how TLS is configured on that endpoint to ensure weak protocols or outdated ciphers aren't allowed, and that certificates are valid and trusted. Describing the target as the host device emphasizes the end point being tested, rather than the client that connects, the network path, or the service role alone. While a server can host TLS, the broader term host device is the precise target PCI scans use to cover any device providing TLS services.*

## 9. It is compulsory to submit scan report results according to each payment brand's compliance reporting requirements.

A. SOMETIMES

B. CANNOT BE DETERMINED

C. TRUE

D. FALSE

*Submitting scan results to meet payment brand reporting requirements is mandatory because external vulnerability scans are part of PCI DSS validation. The standard requires quarterly scans by an Approved Scanning Vendor and, crucially, that the results are shared with the entities responsible for validating compliance—typically the acquiring bank or the payment brands—in the format and within the timelines each brand specifies. This process lets brands verify that vulnerabilities are being identified and remediated on an ongoing basis. Not submitting according to brand requirements can jeopardize PCI compliance and expose you to penalties, so the statement is true.*

SAMPLE

## 10. QIR stands for what?

A. Qualified Internal Reviewer

B. Qualified Incident Responder

C. Qualified Information Resource

D. Qualified Integrator Reseller

*In PCI terms, QIR refers to the Qualified Integrator and Reseller program. This designation applies to organizations that install, integrate, or resell payment applications and related solutions, with an emphasis on ensuring they are trained and validated to deploy these systems securely so they don't compromise cardholder data. The option that best fits this concept is the one that includes both roles: integrator and reseller. The other choices describe different functions (internal reviewer, incident responder, information resource) that do not align with the PCI QIR program's focus on secure installation and integration of payment applications.*

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://pciasvonline.examzify.com

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

SAMPLE