PCI Approved Scanning Vendor (ASV) Online 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. **Entities with existing SSL/early TLS implementations must have what in place?**

   A. A formal Risk Mitigation and Migration Plan.

   B. A plan to disable TLS immediately.

   C. A quarterly vulnerability scan by ASV.

   D. No action required.

2. **The note indicates that vulnerability assessments for public-facing web applications are not the same as vulnerability scans performed for Requirement 11.2. Which statement best describes this distinction?**

   A. They are the same processes

   B. They are separate processes with different scopes

   C. 11.2 scans are optional for public-facing apps

   D. 11.2 scans are more frequent than annual assessments

3. **Which item is not listed as a Special Note?**

   A. When POS software is detected

   B. When remote access software is detected

   C. When directory browsing on a web server is detected

   D. When antivirus software is detected

4. **Which statement addresses documentation and business justification and approval for use of all services, protocols, and ports allowed?**

   A. Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

   B. Documentation and business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.

   C. Prohibit direct public access between Internet and any system component in the cardholder data environment.

   D. Limit inbound Internet traffic to IP addresses within the DMZ.

5. Which of the following is a Special Note defined by the Program Guide when detected?

A. When directory browsing on a web server is detected

B. When POS software is detected

C. When remote access software is detected

D. When the environment behind load balancers cannot be shown

6. Which statement prohibits direct public access between the Internet and any system component in the cardholder data environment?

A. Prohibit direct public access between the Internet and any system component in the cardholder data environment.

B. Limit inbound Internet traffic to IP addresses within the DMZ.

C. Implement anti-spoofing measures to detect and block forged source IP addresses.

D. Documentation and business justification and approval for use of all services, protocols, and ports allowed.

7. Which PCI DSS program is associated with Cardholder Information Security Program?

A. Visa Inc

B. Visa Europe

C. Mastercard

D. Discover

8. What are the 3 sections of the CVSS Environmental, Impact Subscore Modifiers Metric?

A. Confidentiality Requirement; Integrity Requirement; Availability Requirement

B. Confidentiality Impact; Integrity Impact; Availability Impact

C. Access Vector; Attack Complexity; Privileges Required

D. Confidentiality Requirement; Integrity; Availability

9. What does requirement 8.2 require regarding credentials?

A. Render credentials unreadable during transmission and storage

B. Store credentials in plaintext

C. Use symmetric encryption only

D. Do not encrypt at all

10. Which SAQ applies to a merchant with only card-present dial-out terminals?

A. SAQ B

B. SAQ A

C. SAQ C

D. SAQ P2PE

Answers

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

Explanations

1. **Entities with existing SSL/early TLS implementations must have what in place?**

   A. A formal Risk Mitigation and Migration Plan.

   B. A plan to disable TLS immediately.

   C. A quarterly vulnerability scan by ASV.

   D. No action required.

When SSL and early TLS are still in use, the key idea is actively managing the risk they pose and planning how to move to stronger cryptography. The required approach is to have a formal risk mitigation and migration plan that documents the identified risks from continuing to rely on these older protocols, outlines a concrete path to disable or migrate away from them, and sets timelines, milestones, and ownership for the remediation. This plan shows governance and accountability to auditors, proving that the organization is not leaving payment data exposed and that steps are in place to reduce risk in a controlled, auditable way. It's not enough to rely on scans alone, or to try to disable TLS immediately without a structured transition. A vulnerability scan helps identify issues, but it doesn't provide the planned, phased approach, responsibilities, and timing needed to safely retire deprecated protocols. And doing nothing is obviously not acceptable when there's a known risk.

2. **The note indicates that vulnerability assessments for public-facing web applications are not the same as vulnerability scans performed for Requirement 11.2. Which statement best describes this distinction?**

   A. They are the same processes

   B. They are separate processes with different scopes

   C. 11.2 scans are optional for public-facing apps

   D. 11.2 scans are more frequent than annual assessments

The key idea is that these are two distinct activities with different targets and timing. A vulnerability assessment for public-facing web applications focuses on the web app itself—its code, configurations, input handling, authentication, session management, and other application-layer risks that an exposed internet-facing interface can reveal. It looks for flaws that allow attackers to exploit the application directly, and it is treated as a separate, dedicated assessment for PFWA. Vulnerability scans for Requirement 11.2, on the other hand, are broader scans of the underlying infrastructure—networks, servers, and devices that support in-scope systems. They aim to identify vulnerabilities at the network/host level and are performed on a more frequent cadence (quarterly and after significant changes). Because of the different focus (application-layer risks versus infrastructure risks) and the different cadence, these activities are separate processes. So, the best statement is that they are separate processes with different scopes. The other choices either imply they're the same, rely on an incorrect assumption about optionality, or focus only on frequency without acknowledging the distinct scope.

3. Which item is not listed as a Special Note?

A. When POS software is detected

B. When remote access software is detected

C. When directory browsing on a web server is detected

D. When antivirus software is detected

Special Notes in an ASV scan are flags for conditions that need human review or fall outside the standard automated checks, often related to risky configurations or software that could indicate non-compliance. Examples like POS software being detected, remote access software being detected, or directory listing enabled on a web server signal scenarios that require careful interpretation and remediation planning. These are situations where the scan report prompts you to verify that the environment meets PCI DSS requirements. Antivirus software detection, however, is a baseline security control—having antivirus installed and up to date is a standard expectation under PCI DSS. It isn't a conditional or unusual finding that requires the special note type of review; if antivirus is present, there's typically no special note triggered. If antivirus is missing or out of date, that would be addressed as a separate vulnerability finding rather than a Special Note.

4. Which statement addresses documentation and business justification and approval for use of all services, protocols, and ports allowed?

A. Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

B. Documentation and business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.

C. Prohibit direct public access between Internet and any system component in the cardholder data environment.

D. Limit inbound Internet traffic to IP addresses within the DMZ.

The main idea here is governance and change control over what services, protocols, and ports are allowed in the environment. The best statement explicitly requires documenting the business justification and obtaining formal approval for every service, protocol, and port that is allowed, and it also calls for documenting the security features in place for protocols that are considered insecure. This creates an auditable process: you only enable what has a documented business need, and you address the risks of insecure protocols with stated security controls. That combination—approval, justification, and documented mitigations—directly addresses how permissions for network services should be managed, which is essential for PCI compliance. The other options describe protective network configurations (restrict connections, prohibit direct Internet access, limit inbound traffic to a DMZ) but they don't emphasize the documented business justification and approval process for all allowed services and protocols, which is what this item is testing.

5. Which of the following is a Special Note defined by the Program Guide when detected?

A. When directory browsing on a web server is detected

B. When POS software is detected

C. When remote access software is detected

D. When the environment behind load balancers cannot be shown

Special Notes in the PCI ASV Program Guide are used to flag conditions that require special handling during an external vulnerability scan. When POS software is detected, that situation triggers a Special Note. This is because POS environments often involve isolated devices or vendor-specific software that may not be fully testable by standard scanning tools, so the note ensures the assessor documents and accounts for these nuances—sometimes indicating the need for manual verification or adjusted scope. The other conditions listed—directory listing on a web server, detection of remote access software, or environments behind load balancers whose details can't be shown—aren't defined as Special Notes in this context, so they don't carry the same formal flag.

6. Which statement prohibits direct public access between the Internet and any system component in the cardholder data environment?

A. Prohibit direct public access between the Internet and any system component in the cardholder data environment.

B. Limit inbound Internet traffic to IP addresses within the DMZ.

C. Implement anti-spoofing measures to detect and block forged source IP addresses.

D. Documentation and business justification and approval for use of all services, protocols, and ports allowed.

The main idea is to keep the cardholder data environment from being directly reachable from the Internet. This ensures something inside the CDE cannot be accessed with a single, direct Internet connection, reducing exposure to external threats. The statement that directly prohibits Internet access to any system component in the CDE aligns with the goal of network segmentation and layered defenses: public-facing services can sit in a DMZ or similar boundary, but the internal systems containing cardholder data must not be exposed to the Internet without passing through controlled security controls. Why this is the best fit: it states an explicit prohibition of direct public access from the Internet to any CDE component, which is exactly what you need to minimize risk and comply with PCI DSS guidance on isolating the CDE from direct Internet exposure. Why the other options don't fit: limiting inbound traffic to DMZ addresses improves security but does not inherently prohibit direct access to systems inside the CDE; you could still have a direct path from Internet to internal components if rules aren't configured perfectly. Anti-spoofing helps verify legitimate sources, not the presence of direct Internet paths to the CDE. Documentation and approvals govern what services are allowed, not the fundamental rule about direct Internet access to CDE components.

7. Which PCI DSS program is associated with Cardholder Information Security Program?

A. Visa Inc

B. Visa Europe

C. Mastercard

D. Discover

Cardholder Information Security Program is Visa's security program for protecting Visa card data. It's a Visa-specific set of requirements that merchants and service providers handling Visa transactions must meet, and it's distinct from other networks' programs. Because CISP is tied to Visa, the correct association is Visa Inc. Mastercard and Discover have their own security programs, not CISP, and PCI DSS serves as the universal baseline across networks.

8. What are the 3 sections of the CVSS Environmental, Impact Subscore Modifiers Metric?

A. Confidentiality Requirement; Integrity Requirement; Availability Requirement

B. Confidentiality Impact; Integrity Impact; Availability Impact

C. Access Vector; Attack Complexity; Privileges Required

D. Confidentiality Requirement; Integrity; Availability

In CVSS, the Environmental metrics include modifiers that tailor the impact of a vulnerability to a specific environment. The three sections that make up the Impact Subscore Modifiers are Confidentiality Requirement, Integrity Requirement, and Availability Requirement. These modifiers indicate how critical each security property is to the organization, and they adjust the impact score accordingly (for example, making confidentiality more or less impactful depending on how important it is in that environment). The other options mix up terms from different parts of CVSS: one lists the actual impact metrics (Confidentiality Impact, Integrity Impact, Availability Impact) rather than the environmental modifiers; another lists exploitability factors (Access Vector, Attack Complexity, Privileges Required); and the last option blends some correct terms with missing wording (Integrity and Availability without the "Requirement" qualifier).

9. What does requirement 8.2 require regarding credentials?

A. Render credentials unreadable during transmission and storage

B. Store credentials in plaintext

C. Use symmetric encryption only

D. Do not encrypt at all

Protecting credentials means ensuring they cannot be read by anyone who isn't authorized. Requirement 8.2 asks you to render credentials unreadable during both transmission and storage. In practice, this means encrypting data as it moves across networks (like using TLS) and protecting stored credentials with strong cryptographic measures (for passwords, this often involves hashing with salt, and for other secrets or keys, encrypting them with protected keys and proper key management). The goal is that even if data is captured or accessed, the information remains unintelligible to unauthorized parties. Storing credentials in plaintext, relying only on symmetric encryption without broader protection, or not encrypting at all would fail to meet this requirement because they leave sensitive data readable or vulnerable.

10. Which SAQ applies to a merchant with only card-present dial-out terminals?

A. SAQ B

B. SAQ A

C. SAQ C

D. SAQ P2PE

This question tests PCI DSS scope—which SAQ fits when you truly only have card-present, dial-out terminals that connect to the processor and you don't store cardholder data electronically on your systems. In this setup, the merchant's environment is limited to the physical terminals and the dial path to the processor, with no CHD stored on the merchant's devices or networks. That configuration is precisely what the SAQ designed for card-present dial-out devices covers. The reason this is the best fit is that SAQ categories are defined by how card data is handled and where it's stored or processed. A setup with only standalone, dial-out card-present terminals falls under a category that assumes no electronic storage of CHD on the merchant's systems and no internet-connected payment applications, focusing controls on protecting those terminals and the direct connection to the processor. The other options don't align with this scenario. A card-not-present outsourced model involves processing that occurs externally and typically targets merchants that do not handle CHD electronically or that rely entirely on hosted solutions for card-not-present transactions. An internet-connected POS scenario would require an SAQ that accounts for online or networked POS components. A P2PE approach presumes the use of a validated point-to-point encryption solution, which changes the data flow and scope beyond a simple dial-out terminal environment.

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!