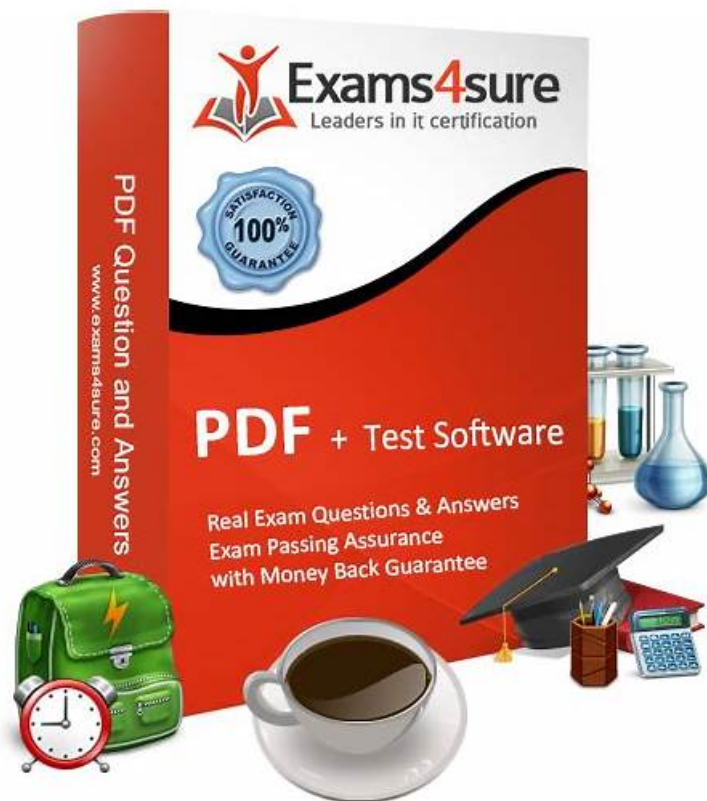


Confused About Where to Start Your PCI SSC QSA_New_V4 Exam Preparation? Here's What You Need to Know



BTW, DOWNLOAD part of Prep4SureReview QSA_New_V4 dumps from Cloud Storage: <https://drive.google.com/open?id=1zwrSbFHeZ5d24I6vQengELSNcxqRKWhH>

The software is designed for use on a Windows computer. This software helps hopefuls improve their performance on subsequent attempts by recording and analyzing Qualified Security Assessor V4 Exam (QSA_New_V4) exam results. Like the actual PCI SSC QSA_New_V4 Certification Exam, Qualified Security Assessor V4 Exam (QSA_New_V4) practice exam software has a certain number of questions and allocated time to answer.

PCI SSC QSA_New_V4 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• PCI Validation Requirements: This section of the exam measures the skills of Compliance Analysts and evaluates the processes involved in validating PCI DSS compliance. Candidates must understand the different levels of merchant and service provider validation, including self-assessment questionnaires and external audits. One essential skill tested is determining the appropriate validation method based on business type.
Topic 2	<ul style="list-style-type: none">• PCI Reporting Requirements: This section of the exam measures the skills of Risk Management Professionals and covers the reporting obligations associated with PCI DSS compliance. Candidates must be able to prepare and submit necessary documentation, such as Reports on Compliance (ROCs) and Self-Assessment Questionnaires (SAQs). One critical skill assessed is compiling and submitting accurate PCI compliance reports.

Topic 3	<ul style="list-style-type: none"> • Payment Brand Specific Requirements: This section of the exam measures the skills of Payment Security Specialists and focuses on the unique security and compliance requirements set by different payment brands, such as Visa, Mastercard, and American Express. Candidates must be familiar with the specific mandates and expectations of each brand when handling cardholder data. One skill assessed is identifying brand-specific compliance variations.
Topic 4	<ul style="list-style-type: none"> • PCI DSS Testing Procedures: This section of the exam measures the skills of PCI Compliance Auditors and covers the testing procedures required to assess compliance with the Payment Card Industry Data Security Standard (PCI DSS). Candidates must understand how to evaluate security controls, identify vulnerabilities, and ensure that organizations meet compliance requirements. One key skill evaluated is assessing security measures against PCI DSS standards.
Topic 5	<ul style="list-style-type: none"> • Real-World Case Studies: This section of the exam measures the skills of Cybersecurity Consultants and involves analyzing real-world breaches, compliance failures, and best practices in PCI DSS implementation. Candidates must review case studies to understand practical applications of security standards and identify lessons learned. One key skill evaluated is applying PCI DSS principles to prevent security breaches.

>> Latest QSA_New_V4 Test Voucher <<

QSA_New_V4 Reliable Test Preparation, Test QSA_New_V4 Sample Online

These experts are committed and work together and verify each QSA_New_V4 exam question so that you can get the real, valid, and updated Qualified Security Assessor V4 Exam (QSA_New_V4) exam practice questions all the time. So you do not need to get worried, countless QSA_New_V4 exam candidates have already passed their dream PCI SSC QSA_New_V4 Certification Exam and they all got help from real, valid, and error-free QSA_New_V4 exam practice questions. So you also need to think about your future and advance your career with the badge of QSA_New_V4 certification exam.

PCI SSC Qualified Security Assessor V4 Exam Sample Questions (Q65-Q70):

NEW QUESTION # 65

If an entity shares cardholder data with a TPSP, what activity is the entity required to perform?

- A. The entity must test the TPSP's incident response plan at least quarterly.
- **B. The entity must monitor the TPSP's PCI DSS compliance status at least annually.**
- C. The entity must perform a risk assessment of the TPSP's environment at least quarterly.
- D. The entity must conduct ASV scans on the TPSP's systems at least annually.

Answer: B

Explanation:

PCI DSS Requirement 12.8.4 mandates that an entity monitor the compliance status of third-party service providers (TPSPs) at least annually, especially when those TPSPs store, process, or transmit account data on the entity's behalf.

* Option A: Incorrect. Entities are not responsible for conducting ASV scans on TPSPs.

* Option B: Incorrect. There is no quarterly risk assessment requirement for TPSPs.

* Option C: Incorrect. Incident response testing for TPSPs is not a direct responsibility of the entity.

* Option D: Correct. Annual monitoring of TPSP compliance is explicitly required.

NEW QUESTION # 66

What must the assessor verify when testing that PAN is protected whenever it is sent over the Internet?

- A. The security protocol is configured to accept all digital certificates.
- **B. The PAN is encrypted with strong cryptography.**
- C. The PAN is securely deleted once the transmission has been sent.
- D. The security protocol is configured to support earlier versions.

Answer: B

Explanation:

Under Requirement 4.2.1.1, PAN (Primary Account Number) must be protected using strong cryptography whenever it is transmitted over open, public networks, including the Internet. Assessors are expected to verify that the cryptographic protocols (e.g., TLS 1.2 or higher) are properly implemented and that weak protocols (e.g., SSL, early TLS) are disabled.

- * Option A#Incorrect. Supporting earlier protocol versions (e.g., SSL, TLS 1.0) is non-compliant.
- * Option B#Correct. Strong encryption (e.g., AES over TLS 1.2 or higher) must be verified.
- * Option C#Incorrect. Accepting all certificates could allow MITM (Man-in-the-Middle) attacks.
- * Option D#Incorrect. Deleting PAN after transmission is not a substitute for protecting it during transmission.

References:

PCI DSS v4.0.1 - Requirement 4.2.1.1

PCI DSS Glossary - Definitions for "strong cryptography" and "open, public networks"

NEW QUESTION # 67

The Intent of assigning a risk ranking to vulnerabilities Is to?

- A. Prioritize the highest risk items so they can be addressed more quickly.
- B. Ensure all vulnerabilities are addressed within 30 days.
- C. Replace the need for quarterly ASV scans.
- D. Ensure that critical security patches are installed at least quarterly

Answer: A

Explanation:

Intent of Risk Ranking

- * PCI DSS Requirement 6.3.2 requires that entities assign a risk ranking to vulnerabilities to prioritize remediation efforts.
- * This ensures that the most critical vulnerabilities are addressed in a timely manner, reducing the risk to the CDE.

Practical Implementation

- * Vulnerabilities are assessed based on potential impact and likelihood of exploitation, typically using industry-standard frameworks like CVSS.
- * High-risk vulnerabilities may require immediate attention, while lower-priority issues are remediated per schedule.

Incorrect Options

- * Option A: PCI DSS does not mandate a 30-day remediation window for all vulnerabilities; remediation timelines depend on risk.
- * Option B: Quarterly ASV scans are still required even with risk ranking.
- * Option D: Installing patches quarterly does not align with the dynamic prioritization of risks.

NEW QUESTION # 68

What process is required by PCI DSS for protecting card-reading devices at the point-of-sale?

- A. Device identifiers and security labels are periodically replaced.
- B. Devices are periodically inspected to detect unauthorized card skimmers.
- C. Devices are physically destroyed if there is suspicion of compromise.
- D. The serial number of each device is periodically verified with the device manufacturer.

Answer: B

Explanation:

Requirement 9.9.2 of PCI DSS v4.0.1 mandates that entities regularly inspect POS devices to detect signs of tampering or skimming. This includes physical inspections to identify unexpected additions, unauthorized stickers, broken seals, etc.

- * Option A: Correct. Regular inspection for skimming/tampering is required.
- * Option B: Incorrect. There is no mandate for manufacturer serial number verification.
- * Option C: Incorrect. PCI DSS does not require routine replacement of device identifiers or labels.
- * Option D: Incorrect. Devices may be investigated if compromised, but not necessarily destroyed.

NEW QUESTION # 69

Which statement about the Attestation of Compliance (AOC) is correct?

- Answer: B**

* Option D: Incorrect. Both the entity and the assessor (if applicable) must sign.

• • • • •

[illegible]

myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, pixabay.com, www.stes.tyc.edu.tw, bbs.t-firefly.com,
www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest Prep4SureReview QSA_New_V4 PDF dumps from Cloud Storage for free:
<https://drive.google.com/open?id=1zwrSbFHeZ5d24I6vQengELSNcxqRKWhH>