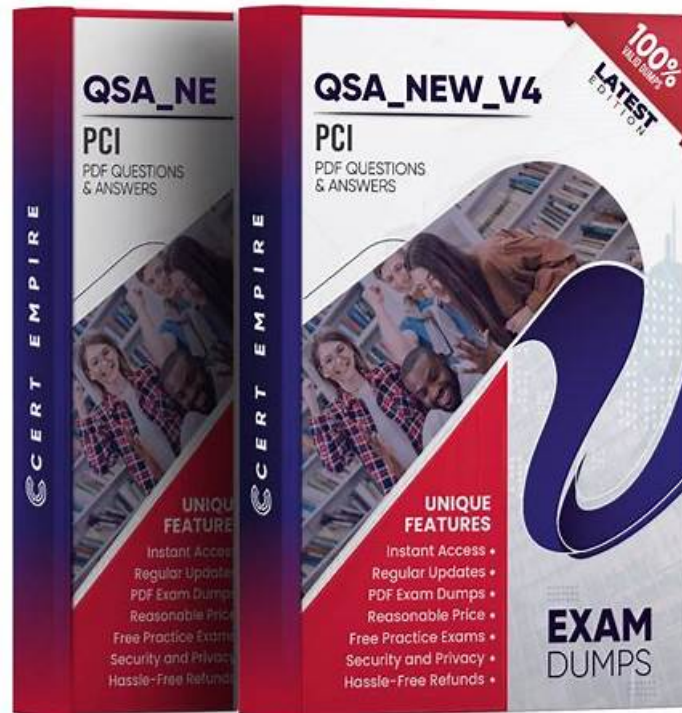


Testking QSA_New_V4 Exam Questions - QSA_New_V4 Training Materials



P.S. Free & New QSA_New_V4 dumps are available on Google Drive shared by DumpStillValid: <https://drive.google.com/open?id=1bHFZ0v77fxRvstqof8eFVCupcOgsj7yi>

With a high quality, we can guarantee that our QSA_New_V4 practice quiz will be your best choice. There are three different versions of our QSA_New_V4 guide dumps: the PDF, the software and the online. The three versions of our QSA_New_V4 learning engine are all good with same questions and answers. Our products have many advantages, I am going to introduce you the main advantages of our QSA_New_V4 Study Materials, I believe it will be very beneficial for you and you will not regret to use our products.

Have you ever used DumpStillValid PCI SSC QSA_New_V4 Dumps? The braindump is latest updated certification training material, which includes all questions in the real exam that can 100% guarantee to pass your exam. These real questions and answers can lead to some really great things. If you fail the exam, we will give you FULL REFUND. DumpStillValid practice test materials are used with no problem. Using DumpStillValid exam dumps, you will achieve success.

>> Testking QSA_New_V4 Exam Questions <<

PCI SSC - High Pass-Rate Testking QSA_New_V4 Exam Questions

This PCI SSC PDF file is a really convenient and manageable format. Furthermore, the PCI SSC QSA_New_V4 PDF is printable which enables you to study or revise questions on the go. This can be helpful since staring at a screen during long study hours can be tiring and the QSA_New_V4 PDF hardcopy format is much more comfortable. And this Qualified Security Assessor V4 Exam price is affordable.

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"> • 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.
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"> • 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.

PCI SSC Qualified Security Assessor V4 Exam Sample Questions (Q36-Q41):

NEW QUESTION # 36

What must be included in an organization's procedures for managing visitors?

- A. Visitors retain their identification (for example, a visitor badge) for 30 days after completion of the visit.
- B. Visitor badges are identical to badges used by onsite personnel.
- C. Visitor log includes visitor name, address, and contact phone number.
- **D. Visitors are escorted at all times within areas where cardholder data is processed or maintained.**

Answer: D

Explanation:

According to Requirement 9.4.2.2, visitors must be escorted at all times in areas where cardholder data is stored or processed. This is a key component of physical access control and is intended to prevent unauthorized access or tampering.

* Option A: #Correct. Escorts are mandatory for visitors in sensitive areas.

* Option B: #Incorrect. Visitor badges must be distinguishable from employee badges.

* Option C: #Incorrect. PCI DSS requires name and firm represented, but not full address or phone.

* Option D: #Incorrect. Visitor badges must be surrendered or deactivated immediately after the visit ends.

NEW QUESTION # 37

Which statement is true regarding the PCI DSS Report on Compliance (ROC)?

- **A. The ROC Reporting Template and instructions provided by PCI SSC should be used for all ROCs.**
- B. The ROC Reporting Template provided by PCI SSC is only required for service provider assessments.
- C. The assessor must create their own ROC template for each assessment report.
- D. The assessor may use either their own template or the ROC Reporting Template provided by PCI SSC.

Answer: A

NEW QUESTION # 38

The intent of assigning a risk ranking to vulnerabilities is to?

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

Answer: C

Explanation:

PCI DSS Requirement 6.3.1 requires entities to assign a risk ranking to vulnerabilities (e.g., high, medium, low) to ensure that remediation efforts are prioritised. This risk-based approach helps organisations focus resources where they are most needed.

* Option A: Incorrect. Timeframes depend on the severity and internal policy, not always 30 days.

* Option B: Incorrect. Risk ranking supports remediation but doesn't replace scanning.

* Option C: Correct. The purpose is to prioritise higher-risk items for faster action.

* Option D: Incorrect. Patch frequency is addressed elsewhere (Requirement 6.3.3).

NEW QUESTION # 39

Where an entity under assessment is using the customized approach, which of the following steps is the responsibility of the assessor?

- A. Derive testing procedures and document them in Appendix E of the ROC.
- B. Monitor the control.
- C. Perform the targeted risk analysis as per PCI DSS requirement 12.3.2.
- **D. Document and maintain evidence about each customized control as defined in Appendix E of PCI DSS.**

Answer: D

Explanation:

Customized Approach Overview

* Appendix E of PCI DSS v4.0 outlines the customized approach, which allows entities to demonstrate their control effectiveness using methods that differ from the defined approach.

Assessor Responsibilities

* QSAs must document and maintain detailed evidence for each customized control implemented by the entity.

* Evidence must support how the customized control meets the security objectives of the original requirement.

Testing and Validation

* The QSA must perform validation to confirm the customized control's adequacy and effectiveness and ensure it sufficiently addresses the requirement's intent.

Documentation

* All findings, testing procedures, and conclusions must be recorded in the Report on Compliance (ROC) Appendix E, providing traceability and transparency.

NEW QUESTION # 40

Which statement is true regarding the use of intrusion detection techniques, such as intrusion detection systems and/or intrusion protection systems (IDS/IPS)?

- A. Intrusion detection techniques are required on all system components.
- B. Intrusion detection techniques are required to isolate systems in the cardholder data environment from all other systems.
- **C. Intrusion detection techniques are required to alert personnel of suspected compromises.**
- D. Intrusion detection techniques are required to identify all instances of cardholder data.

Answer: C

Explanation:

Requirement 11.5.1 mandates that organisations deploy intrusion-detection or prevention tools to monitor traffic and generate alerts for

Reference:PCI DSS v4.0.1 - Requirement 11.5.1.

• • • • •

QSA New V4 Training Materials: <https://www.dumpstillvalid.com/QSA-New-V4-prep4sure-review.html>

- BTW, DOWNLOAD part of DumpStillValid QSA_New_V4 dumps from Cloud Storage: <https://drive.google.com/open?id=1bHFZ0v77fRvstqof8eFVCupcOgsj7yi>

