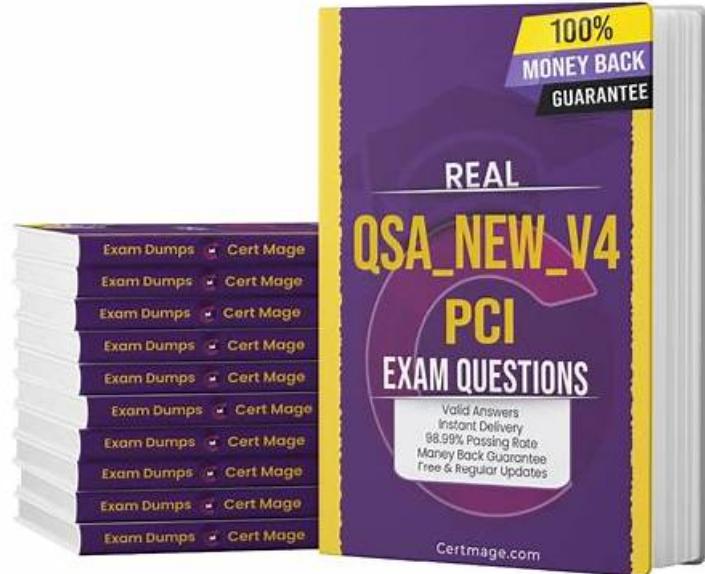


Three Easy-to-Use and Compatible ValidDumps PCI SSC QSA_New_V4 Exam Questions



BTW, DOWNLOAD part of ValidDumps QSA_New_V4 dumps from Cloud Storage: <https://drive.google.com/open?id=1PPLDFT2Lqiu59wm1Uxd6QcThe1CGbF9A>

Our passing rate is 98%-100% and there is little possibility for you to fail in the exam. But if you are unfortunately to fail in the exam we will refund you in full immediately. Some people worry that if they buy our QSA_New_V4 exam questions they may fail in the exam and the procedure of the refund is complicated. But we guarantee to you if you fail in we will refund you in full immediately and the process is simple. If only you provide us the screenshot or the scanning copy of the QSA_New_V4 failure marks we will refund you immediately. If you have doubts or other questions please contact us by emails or contact the online customer service and we will reply you and solve your problem as quickly as we can. So feel relieved when you buy our QSA_New_V4 guide torrent.

PCI SSC QSA_New_V4 Exam Syllabus Topics:

Topic	Details
Topic 1	<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 2	<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 3	<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 4	<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 5	<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.

>> Certification QSA_New_V4 Dump <<

QSA_New_V4 Actualtest, QSA_New_V4 New Practice Questions

With our QSA_New_V4 training braindumps, you must feel respected. We believe that every individual has his or her own will, and we will not force you to make any decision. What we can do is to make our QSA_New_V4 learning prep perfect as much as possible, and let our QSA_New_V4 practice quiz conquer you with your own charm. And there are three versions of the QSA_New_V4 exam questions: the PDF, Software and APP online which you can choose as you like.

PCI SSC Qualified Security Assessor V4 Exam Sample Questions (Q57-Q62):

NEW QUESTION # 57

An organization has implemented a change-detection mechanism on their systems. How often must critical file comparisons be performed?

- A. Only after a valid change is installed
- B. At least monthly
- C. Periodically as defined by the entity
- D. At least weekly**

Answer: D

Explanation:

As specified under Requirement 11.5.2.1, comparisons of critical files (e.g., config files, executables) using change-detection mechanisms (e.g., FIM tools) must occur at least weekly. This ensures timely detection of unauthorized changes or tampering.

* Option A:#Correct. Weekly is the minimum frequency required.

* Option B:#Incorrect. A defined "period" is not sufficient unless it's weekly or more frequent.

* Option C:#Incorrect. Scans should not wait for changes; they should detect unexpected ones.

* Option D:#Incorrect. Monthly is too infrequent for PCI DSS compliance.

NEW QUESTION # 58

Passwords for default accounts and default administrative accounts should be?

- A. Changed before installing a system on the network.**
- B. Reset to the default password before installing a system on the network.
- C. Changed within 30 days after installing a system on the network.
- D. Configured to expire in 30 days.

Answer: A

Explanation:

According to Requirement 2.2.6, default passwords must be changed before systems are installed on the network. The use of default credentials (such as "admin/admin") presents a major security risk and is a well-known vector for breaches.

- * Option A: Incorrect. Changing within 30 days is not soon enough per PCI DSS.
- * Option B: Incorrect. Resetting to default would defeat the purpose of secure configuration.
- * Option C: Correct. The requirement is to change default passwords prior to network connection.
- * Option D: Incorrect. Password expiration policies are a separate topic under Requirement 8.

References:

PCI DSS v4.0.1 - Requirement 2.2.6;
PCI DSS v4.0.1 - Guidance for Requirement 2.2.6.

NEW QUESTION # 59

According to Requirement 1, what is the purpose of "Network Security Controls"?

- A. Control network traffic between two or more logical or physical network segments.
- B. Encrypt PAN when stored.
- C. Discover vulnerabilities and rank them
- D. Manage anti-malware throughout the CDE.

Answer: A

Explanation:

According to Requirement 1.2.1 of PCI DSS v4.0.1, network security controls (NSCs), such as firewalls and segmentation controls, are used to restrict and control traffic between trusted and untrusted networks. This includes logical or physical network segmentation.

- * Option A: Incorrect. Anti-malware is addressed in Requirement 5.
- * Option B: Correct. NSCs control and restrict inbound and outbound traffic between logical and physical network segments.
- * Option C: Incorrect. Vulnerability management is under Requirement 6.
- * Option D: Incorrect. PAN encryption is covered in Requirement 3.5.

NEW QUESTION # 60

A sample of business facilities is reviewed during the PCI DSS assessment. What is the assessor required to validate about the sample?

- A. It includes a consistent set of facilities that are reviewed for all assessments.
- B. The number of facilities in the sample is at least 10 percent of the total number of facilities.
- C. All types and locations of facilities are represented.
- D. Every facility where cardholder data is stored is reviewed.

Answer: C

Explanation:

Per Section 6 - Sampling for PCI DSS Assessments, the assessor must ensure the sample of business facilities includes all types and locations, reflecting different operational environments. The goal is to cover variations that might affect compliance, such as data centers vs. call centers, or regional differences.

- * Option A: Incorrect. Each assessment may require a different sample depending on the environment.
- * Option B: Incorrect. There is no fixed 10% requirement for facility sampling.
- * Option C: Incorrect. A full review of every facility isn't required if representative sampling is used appropriately.
- * Option D: Correct. The sampling must include all types and locations of facilities to be valid.

NEW QUESTION # 61

Which systems must have anti-malware solutions?

- A. All portable electronic storage.
- B. All systems that store PAN.
- C. All CDE systems, connected systems, NSCs, and security-providing systems.
- D. Any in-scope system except for those identified as 'not at risk' from malware.

Answer: D

Explanation:

Requirement 5.2.1.1 clarifies that anti-malware solutions are required on all in-scope systems, unless the system is evaluated as not at risk for malware (e.g., Linux-based appliances with no Internet access). These risk evaluations must be documented and justified (5.2.3.1).

- * Option A:#Incorrect. PCI DSS allows exceptions for systems not at risk.
- * Option B:#Incorrect. Anti-malware applies to systems, not portable media per se.
- * Option C:#Incorrect. Anti-malware scope is broader than just PAN-storing systems.
- * Option D:#Correct. Systems not at risk can be excluded if justified and documented.

Reference:PCI DSS v4.0.1 - Requirement 5.2.1.1 and 5.2.3.1.

NEW QUESTION # 62

• • • • •

As is known to us, perfect after-sales service for buyers is a very high value. Our QSA_New_V4 Guide Torrent not only has the high quality and efficiency but also the perfect service system after sale. Our QSA_New_V4 exam questions can help you save much time, if you use our products, you just need to spend 20-30 hours on learning, and you will pass your exam successfully. What most important is that you can download our study materials about 5~10 minutes after you purchase.

QSA_New_V4 Actualtest: https://www.validdumps.top/QSA_New_V4-exam-torrent.html

What's more, part of that ValidDumps QSA_New_V4 dumps now are free: <https://drive.google.com/open?id=1PPLDFT2Lqiu59wm1Uxd6OcThe1CGbF9A>