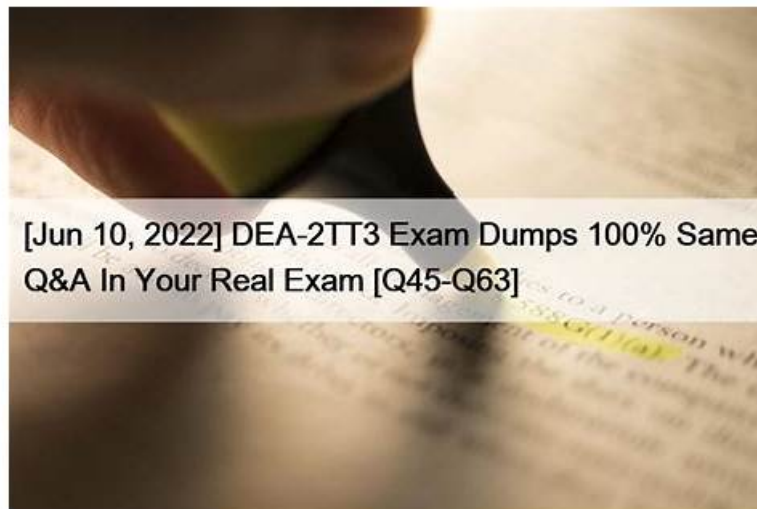


Famous QSA_New_V4 Training Brain Dumps present the most useful Exam Materials - Test4Sure



DOWNLOAD the newest Test4Sure QSA_New_V4 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1481jMWra_ChX2ZSJr1P6-XBQnXeyrV6y

To pass the QSA_New_V4 exam, you must put in a lot of time studying, practicing, and working hard. You will need real PCI SSC QSA_New_V4 Questions and the necessary understanding of the exam's format to pass the QSA_New_V4 test. Without preparing with actual Qualified Security Assessor V4 Exam (QSA_New_V4) questions, applicants find it difficult to get the knowledge essential to pass the PCI SSC certification exam in a short time.

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">• 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 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">• 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 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.
---------	---

>> QSA_New_V4 Reliable Exam Tips <<

PCI SSC QSA_New_V4 exam study materials

In the major environment, people are facing more job pressure. So they want to get QSA_New_V4 certification rise above the common herd. How to choose valid and efficient QSA_New_V4 guide torrent should be the key topic most candidates may concern. So now, it is right, you come to us. Our company is famous for its high-quality in this field especially for QSA_New_V4 Certification exams. After you practice our study materials, you can master the examination point from the QSA_New_V4 exam torrent. Then, you will have enough confidence to pass your exam. We can succeed so long as we make efforts for one thing.

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

NEW QUESTION # 65

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

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

Answer: D

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).

Reference: PCI DSS v4.0.1 - Requirement 6.3.1.

NEW QUESTION # 66

Which of the following describes the intent of installing one primary function per server?

- A. To allow higher-security functions to protect lower-security functions installed on the same server.
- B. To reduce the security level of functions with higher-security needs to meet the needs of lower-security functions.
- C. To allow functions with different security levels to be implemented on the same server.
- **D. To prevent server functions with a lower security level from introducing security weaknesses to higher- security functions on the same server.**

Answer: D

Explanation:

As per Requirement 2.2.1, the purpose of limiting each server to one primary function is to reduce the risk of functions with lower security needs compromising more critical functions.

* Option A: #Incorrect. PCI DSS discourages combining different security-level functions.

* Option B: #Correct. This is the intent: to prevent lower-security processes from weakening high-security environments.

* Option C: #Incorrect. Functions shouldn't depend on one another for security.

* Option D: #Incorrect. PCI DSS encourages raising security, not lowering it.

Reference: PCI DSS v4.0.1 - Requirement 2.2.1.

NEW QUESTION # 67

A network firewall has been configured with the latest vendor security patches. What additional configuration is needed to harden the firewall?

- A. Remove the default 'Firewall Administrator' account and create a shared account for firewall administrators to use.
- B. Synchronize the firewall rules with the other firewalls in the environment.
- **C. Disable any firewall functions that are not needed in production.**
- D. Configure the firewall to permit all traffic until additional rules are defined.

Answer: C

Explanation:

Firewall Hardening:

* Requirement 1.2 mandates that firewalls should be configured with only the necessary functionality to reduce attack surfaces. Disabling unused functions eliminates potential vulnerabilities.

Explanation of Other Options:

* A: Shared accounts violate Requirement 8.1.5, which prohibits shared or generic accounts.

* B: Allowing all traffic initially violates Requirement 1.2.1, which requires a restrictive firewall policy.

* C: Synchronization of rules may not always be necessary, especially for firewalls with different scopes or roles.

NEW QUESTION # 68

An entity wants to know if the Software Security Framework can be leveraged during their assessment. Which of the following software types would this apply to?

- A. Any payment software in the CDE.
- B. Only software which runs on PCI PTS devices.
- C. Validated Payment Applications that are listed by PCI SSC and have undergone a PA-DSS assessment.
- **D. Software developed by the entity in accordance with the Secure SLC Standard.**

Answer: D

Explanation:

Software Security Framework Overview

* PCI SSC's Software Security Framework (SSF) encompasses Secure Software Standard and Secure Software Lifecycle (Secure SLC) Standard.

* Software developed under the Secure SLC Standard adheres to security-by-design principles and can leverage the SSF during PCI DSS assessments.

Applicability

* The framework is primarily for software developed by entities or third parties adhering to PCI SSC standards.

* It does not apply to legacy payment software listed under PA-DSS unless migrated to SSF.

Incorrect Options

* Option A: Not all payment software qualifies; it must align with SSF requirements.

* Option B: PCI PTS devices are subject to different security requirements.

* Option C: PA-DSS-listed software does not automatically meet SSF standards without reassessment.

NEW QUESTION # 69

Which of the following is true regarding compensating controls?

- A. A compensating control worksheet is not required if the acquirer approves the compensating control.
- **B. A compensating control must address the risk associated with not adhering to the PCI DSS requirement.**
- C. A compensating control is not necessary if all other PCI DSS requirements are in place.
- D. An existing PCI DSS requirement can be used as a compensating control if it is already implemented.

Answer: B

Explanation:

Compensating controls are alternative measures implemented when an entity cannot meet a specific PCI DSS requirement due to legitimate technical or business constraints. These controls must sufficiently mitigate the associated risk and be commensurate with

For detailed guidance on compensating controls, refer to Appendix B: Compensating Controls in the PCI DSS v4.0.1 document.

• • • • •

QSA_New_V4 Latest Braindumps Ppt: https://www.test4sure.com/QSA_New_V4-pass4sure-vce.html

- BTW, DOWNLOAD part of Test4Sure QSA_New_V4 dumps from Cloud Storage: https://drive.google.com/open?id=1481jMWra_ChX2ZSJr1P6-XBQnXeyrV6y