DUMPSARENA

Qualified Security Assessor V4 Exam

PCI SSC QSA_New_V4

Version Demo

Total Demo Questions: 9

Total Premium Questions: 95

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which scenario describes segmentation of the cardholder data environment (CDE) for the purposes of reducing PCI DSS scope?

A. Routers that monitor network traffic flows between the CDE and out-of-scope networks.

B. Firewalls that log all network traffic flows between the CDE and out-of-scope networks.

C. Virtual LANs that route network traffic between the CDE and out-of-scope networks.

D. A network configuration that prevents all network traffic between the CDE and out-of-scope networks.

ANSWER: D

Explanation:

A network configuration that prevents all network traffic between the CDE and out-of-scope networks describes segmentation because it creates a clear, enforceable isolation boundary around the cardholder data environment. PCI DSS scope includes the CDE and all system components connected to it, as well as systems that could affect the security of the CDE. Effective network segmentation is not itself a PCI DSS requirement, but it may be used to reduce the number of systems that must be included in the assessment by ensuring that out-of-scope networks cannot connect to, communicate with, or otherwise affect CDE systems.

For segmentation to support a reduced scope determination, the isolation must be implemented through reliable technical controls and validated in the assessment. The boundary should prevent connectivity in both directions unless a specifically authorized and securely controlled path is needed; such permitted paths must be evaluated as part of the CDE boundary. In the scenario stated, preventing all network traffic provides the strongest, unambiguous example of the isolation needed to treat the external network as out of scope. PCI SSC explains the role of segmentation in its network-segmentation scoping FAQ and defines the related scope principles in the PCI DSS v4.0.1.

QUESTION NO: 2

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

A. Monitor the control.

B. Derive testing procedures and document them in Appendix D of the ROC.

C. Document and maintain evidence about each customized control as defined in Appendix E of PCI DSS.

D. Perform the targeted risk analysis as per PCI DSS requirement 12.3.2.

ANSWER: B

Explanation:

Derive testing procedures and document them in Appendix D of the ROC is correct. Under the PCI DSS customized approach, the assessed entity designs and implements a customized control that meets the applicable PCI DSS requirement's objective. The assessor then has an independent validation responsibility: they must develop testing procedures that are appropriate for the specific customized control and sufficient to determine whether the control meets that requirement objective. This cannot be a simple reuse of the defined-approach testing procedure, because the customized control may operate differently from the control described in the standard.

The assessor's testing methodology, test results, and conclusion must be documented in the Report on Compliance's customized-approach appendix. This documentation provides transparency to the entity, its acquirer or payment brands where applicable, and other report users about how the customized control was evaluated. The assessor must also evaluate the entity's customized-approach documentation and targeted risk analysis as part of validating the control, but deriving and recording the assessor-specific test procedures is a defined assessor responsibility. PCI DSS identifies the customized approach in Appendix D and requires assessor testing to validate that the customized control meets the relevant requirement objective. See the PCI SSC Document Library and the PCI SSC PCI DSS overview.

QUESTION NO: 3

An entity allows customer-service personnel to view PAN in a payment application when resolving disputes. The application displays the first eight and last four digits of each PAN to all customer-service personnel. The entity has not documented a business need for displaying more than the first six and last four digits. What should the assessor determine?

A. The display is acceptable because customer-service personnel have a business function.

B. The display is acceptable because the PAN is not being stored in the application.

C. The display does not meet the masking requirement unless a documented business need exists for the additional digits.

D. The display is prohibited because PAN may never be displayed to personnel.

ANSWER: C

Explanation:

The PAN display does not meet the masking requirement as described. When PAN is displayed, it must be masked so that no more than the first six and last four digits are displayed, unless a documented business need exists to see more digits. Access restrictions alone do not remove the masking requirement. The entity must either limit the display to the permitted digits or document and justify the legitimate business need for the additional digits for the applicable roles.

QUESTION NO: 4

Which of the following is a requirement for multi-tenant service providers?

A. Ensure that customers cannot access another entity's cardholder data environment.

B. Provide customers with access to the hosting provider ' s system configuration files.

C. Provide customers with a shared user ID for access to critical system binaries.

D. Ensure that a customer's log files are available to all hosted entities.

ANSWER: A

Explanation:

Ensure that customers cannot access another entity's cardholder data environment. This reflects the core multi-tenant service-provider obligation to maintain effective logical separation between each customer's cardholder data environment (CDE). A multi-tenant provider may use shared infrastructure, but its controls must prevent one hosted entity from viewing, accessing, affecting, or traversing another entity's systems or cardholder data. This separation is not merely a design objective: it must be implemented through appropriate access controls, network segmentation or equivalent isolation mechanisms, and secure tenant administration practices, and it must be supportable with evidence during an assessment.

PCI DSS v4.0.1 addresses this specifically in Appendix A1, Additional PCI DSS Requirements for Multi-Tenant Service Providers. Requirement A1.1 requires the provider to ensure that each customer environment is logically separated from other customer environments so that no customer can access another customer's environment. The assessment procedures further require validation that the separation controls are in place and operating effectively. Therefore, preventing cross-tenant access to another entity's CDE is the applicable requirement. See PCI DSS v4.0.1 and the PCI SSC PCI DSS standards page.

QUESTION NO: 5

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. Configure the firewall to permit all traffic until additional rules are defined.

C. Synchronize the firewall rules with the other firewalls in the environment.

D. Disable any firewall functions that are not needed in production.

ANSWER: D

Explanation:

Disable any firewall functions that are not needed in production is correct because secure firewall hardening requires reducing the device's attack surface in addition to applying current vendor patches. Services, protocols, interfaces, management features, and other functionality that are enabled but unnecessary can create additional paths for compromise, introduce avoidable vulnerabilities, or provide an attacker with capabilities that are not required for the firewall's intended operational role. A hardened production firewall should therefore be configured according to documented business and security requirements, with only the minimum necessary functionality enabled. This applies to both traffic-handling functions and administrative capabilities: unused services should be disabled, and required management access should be deliberately configured and restricted. PCI DSS Requirement 2.2 requires system components to be configured and managed securely, including addressing unnecessary functionality and insecure services, protocols, and daemons. This principle complements the firewall and network-security controls in Requirement 1 by ensuring that the firewall itself is not exposing avoidable services or features. Maintaining vendor patches is essential, but it does not eliminate risks created by unneeded enabled functionality. See the PCI DSS v4.0.1 and the PCI SSC Document Library.

QUESTION NO: 6

An entity wants to use the Customized Approach. They are unsure how to complete the Controls Matrix or TRA. During the assessment, you spend time completing the Controls Matrix and the TRA, while also ensuring that the customized control is implemented securely. Which of the following statements is true?

A. You can assess the customized control, but another assessor must verify that you completed the TRA correctly.

B. You can assess the customized control and verify that the customized approach was correctly followed, but you must document this in the ROC.

C. You must document the work on the customized control in the ROC, but you can not assess the control or the documentation.

D. Assessors are not allowed to assist an entity with the completion of the Controls Matrix or the TRA.

ANSWER: D

Explanation:

Assessors are not allowed to assist an entity with the completion of the Controls Matrix or the TRA. Under the Customized Approach, the entity is responsible for designing its customized control, documenting the control in the Controls Matrix, and performing the targeted risk analysis that supports the control's design and operation. The assessor's role is independent validation: evaluating whether the entity's documented control meets the Customized Approach objective, whether the targeted risk analysis is appropriate, and whether the control is implemented and operating effectively. Completing these artifacts for the entity, or helping design and secure the control during the same assessment, compromises the assessor's independence because the assessor would be validating work they performed or influenced. The entity may obtain appropriate assistance before its assessment, but the assessment must preserve the independence and objectivity required of a QSA. The assessor must then document the Customized Approach assessment procedures, evidence, conclusions, and results in the ROC. PCI SSC's Customized Approach materials and PCI DSS document library describe the entity's responsibilities and the assessor validation process: PCI SSC Customized Approach and PCI SSC Document Library.

QUESTION NO: 7

Which of the following file types must be monitored by a change-detection mechanism (for example, a file-integrity monitoring tool)?

A. Application vendor manuals

B. Files that regularly change

C. Security policy and procedure documents

D. System configuration and parameter files

ANSWER: D

Explanation:

System configuration and parameter files must be monitored by a change-detection mechanism because they can directly affect a system's security configuration, operation, and ability to protect the cardholder data environment. PCI DSS Requirement 11.5.2 requires organizations to deploy a change-detection mechanism, such as file-integrity monitoring, to alert personnel to unauthorized modification of critical files. PCI DSS identifies system configuration files, configuration or parameter files, application executable files, and scripts used for system administration as examples of critical files. An unauthorized alteration to a configuration or parameter file could weaken access controls, logging, network security settings, encryption settings, or other protections that support PCI DSS compliance. The mechanism should therefore establish a trusted baseline for applicable files and generate alerts when unexpected changes are detected, enabling timely investigation and response. The entity defines the specific critical files in scope based on the systems and components in its environment, but system configuration and parameter files are expressly within the category PCI DSS expects to be protected by this control. See PCI SSC's PCI DSS Document Library and the PCI DSS standards overview.

QUESTION NO: 8

At which step in the payment transaction process does the merchant ' s bank pay the merchant for the purchase, and the cardholder ' s bank bill the cardholder?

A. Authorization

B. Clearing

C. Settlement

D. Chargeback

ANSWER: C

Explanation:

Settlement is the payment-transaction stage in which financial obligations arising from cleared card transactions are finalized. Following authorization, which confirms that the transaction may proceed, and clearing, which communicates and reconciles transaction data among the participants, settlement results in the transfer of funds through the payment ecosystem. In practical terms, the acquirer obtains settlement funds through the applicable network process and credits the merchant according to its merchant agreement, while the issuer posts the transaction to the cardholder's account, creating the amount the cardholder must pay under the card account terms. The timing of merchant funding and cardholder statement presentation can vary by acquirer, issuer, card brand, cut-off times, and account arrangements; however, these activities belong to the settlement phase of the standard authorization-clearing-settlement lifecycle. This terminology is also important when assessing payment environments because data and system functions should be understood in the context of how transactions are authorized, cleared, and settled. PCI SSC describes the payment-account-data ecosystem and the entities involved in payment processing in its PCI DSS Quick Reference Guide. A concise overview of the authorization, clearing, and settlement transaction lifecycle is available from the Federal Reserve's card payments resources.

QUESTION NO: 9

Which of the following is true regarding internal vulnerability scans?

A. They must be performed after a significant change.

B. They must be performed by an Approved Scanning Vendor (ASV).

C. They must be performed by QSA personnel.

D. They must be performed at least annually.

ANSWER: A

Explanation:

“They must be performed after a significant change.” is correct because PCI DSS Requirement 11.3.1 requires internal vulnerability scans to be conducted at least once every three months and after significant changes. This requirement ensures that newly introduced or modified components, configurations, network paths, and security controls are assessed for vulnerabilities before they can create an unrecognized exposure in the cardholder data environment. Significant changes can include additions or replacements of system components, changes to network topology, firewall rule modifications, or product upgrades. The organization must also address applicable vulnerabilities in accordance with its risk-ranking process and repeat scans as needed to confirm that high-risk and critical vulnerabilities have been resolved. Internal scanning may be performed by qualified personnel, provided they are organizationally independent of the system or component being scanned, or by a qualified external party. PCI DSS therefore makes post-change internal scanning an explicit ongoing validation activity, rather than limiting it to a fixed periodic schedule. See the PCI SSC Document Library for the current PCI DSS standard and the PCI SSC guidance on significant changes.