PassQueen
a.k.a dumpsqueen.com

ISA-N_RetakePCI Internal Security Assessor Retake

PCI SSC isa-n_retake

Version Demo

Total Demo Questions: 5

Total Premium Questions: 59

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

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: A

Explanation:

Any payment software in the CDE is the applicable choice because the PCI Software Security Framework (SSF) addresses the security of payment software that stores, processes, or transmits payment-account data, or that can affect the security of the cardholder data environment. The framework modernized and succeeded PA-DSS, providing standards that support current payment-software technologies, delivery models, and development methods. Its Secure Software Standard addresses security requirements for qualifying payment software products, while the Secure Software Lifecycle Standard addresses the secure development practices used by software vendors. In a PCI DSS assessment, use of appropriately validated payment software can provide useful assurance that the software has been assessed against applicable SSF security requirements; however, the entity remains responsible for implementing and maintaining PCI DSS controls within its own environment. The relevant consideration is therefore whether the payment software is within, connected to, or security-impacting for the CDE—not whether it operates only on a particular payment-terminal type, was assessed under the retired PA-DSS program, or was developed solely by the assessed entity. PCI SSC describes SSF and its two standards at PCI Software Security Framework and publishes supporting standards and program documentation in its Document Library.

QUESTION NO: 2

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 because unauthorized or unexpected changes to these files can directly alter the security posture and operation of in-scope system components. Under PCI DSS Requirement 11.5.2, change-detection mechanisms such as file-integrity monitoring tools are used to alert personnel to unauthorized modification, addition, or deletion of critical files. The requirement specifically includes system configuration files, configuration parameters, and other critical files, with the monitoring scope defined through the entity's targeted risk analysis. Monitoring these files provides a detective control that helps ensure changes are identified promptly, investigated, and verified as authorized through the organization's change-management processes. This supports the integrity of controls protecting the cardholder data environment, because configuration settings commonly govern authentication, logging, network services, access permissions, and security tooling. The PCI SSC describes file-integrity monitoring as a mechanism for detecting changes to critical system files and configurations. See the PCI SSC Document Library for the current PCI DSS and supporting materials, and PCI SSC's PCI DSS resources for merchants for implementation guidance and program information.

QUESTION NO: 3

An entity maintains a system inventory for its PCI DSS assessment. A newly deployed authentication server does not store, process, or transmit PAN, but it authenticates administrators before they can access CDE systems. The server is absent from the inventory. Which statement is true?

A. The authentication server must be included because it can impact the security of the CDE.

B. The authentication server can be excluded because it does not store, process, or transmit PAN.

C. The authentication server is in scope only when it is located on the same network segment as the CDE.

D. The authentication server can be excluded if it uses multi-factor authentication.

ANSWER: A

Explanation:

The authentication server must be included in the system inventory and evaluated as in scope because it can impact the security of the CDE. PCI DSS scope includes not only system components that store, process, or transmit account data, but also components that can directly affect the security of the CDE.

A compromised or improperly configured authentication server could enable unauthorized administrative access to CDE systems. Therefore, excluding it solely because it does not handle PAN would produce an incomplete inventory and an inaccurate scope determination.

QUESTION NO: 4

Where can live PANs be used for testing?

A. Production (live) environments only

B. Pre-production (test) environments only if located outside the CDE.

C. Pre-production environments that are located within the CDE

D. Testing with live PANs must only be performed in the QSA Company environment

ANSWER: A

Explanation:

Production (live) environments only is correct in the context of PCI DSS v3.2.1. Requirement 6.4.3 requires that production data, including live primary account numbers (PANs), not be used for testing or development. The intent is to ensure that test and development activities do not expose real cardholder data through environments that may have different security controls, less rigorous change control, or broader personnel access than production systems. Where an organization needs to validate payment processing using real cards and live PANs, that activity must occur in the live production environment, which is within scope for PCI DSS and is required to maintain the applicable protections for cardholder data. Such testing must still be carefully authorized, controlled, and monitored so that it does not create unnecessary exposure or interfere with payment processing. The PCI DSS v3.2.1 Quick Reference Guide states the requirement that production data, or live PANs, are not used for testing or development: PCI DSS v3.2.1 Quick Reference Guide. PCI SSC's document library also provides the authoritative PCI DSS standards and supporting materials: PCI SSC Document Library.

QUESTION NO: 5

Passwords for default accounts and default administrative accounts should be?

A. Changed within 30 days after installing a system on the network.

B. Reset to the default password before installing a system on the network

C. Changed before installing a system on the network

D. Configured to expire in 30 days

ANSWER: C

Explanation:

Passwords for default accounts and default administrative accounts should be **changed before installing a system on the network**. Default credentials are widely known, often published in vendor documentation, and commonly targeted by attackers conducting automated scans or attempting unauthorized access. Changing these passwords before a system is connected to the network prevents an exposed device, application, or security component from being accessible with vendor-supplied credentials during initial deployment. This action is part of establishing secure configurations and reducing the risk that an attacker could gain administrative access, alter settings, install malware, or reach systems that store, process, or transmit cardholder data. Under PCI DSS Requirement 2, entities must apply secure configuration standards to system components and change vendor defaults before a system is installed on the network. The requirement applies not only to passwords, but also to other vendor-supplied default security parameters where applicable. The Internal Security Assessor should verify that documented build or deployment procedures require this step and that deployed system configurations demonstrate it has been completed. See the PCI DSS document library and the PCI SSC's guidance on vendor defaults.