PassQueen
a.k.a dumpsqueen.com

Assessor_New_V4 Exam

PCI SSC Assessor_New_V4

Version Demo

Total Demo Questions: 7

Total Premium Questions: 76

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

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. Every facility where cardholder data is stored is reviewed

D. All types and locations of facilities are represented

ANSWER: D

Explanation:

All types and locations of facilities are represented is correct because an assessor's sampling approach must result in a sample that is representative of the full in-scope population. Facilities can differ materially based on their purpose, operational processes, physical environment, technologies, personnel, and geographic location. Those differences may affect how PCI DSS controls are implemented and whether they operate effectively. Selecting facilities across the relevant types and locations provides the assessor with a reasonable basis for determining whether assessment results can be applied to the overall population, rather than only to a narrow or unusually uniform subset.

PCI DSS assessment reporting requires the assessor to document the sampling methodology and the rationale for why the selected sample is representative. The assessor should consider relevant characteristics of the population, including variations in business facilities, and expand or adjust the sample where differences could affect control operation. This is a risk-based professional judgment; it is not a fixed percentage or a requirement to use the same facilities in every assessment. See the PCI SSC PCI DSS Document Library for the current PCI DSS standard and reporting templates, and the PCI SSC Assessors and Solutions resources for assessment-program information.

QUESTION NO: 2

A developer deploys a change to a payment application in production. The change record includes the business reason, documented approval, test results, and a back-out procedure. The change modified database fields, but the data-flow diagram and supporting system documentation were not updated. Which PCI DSS change-control expectation has not been met?

A. The change was not performed during an approved maintenance window

B. The change record did not include an updated data-flow diagram and supporting documentation

C. The developer did not obtain approval from the database vendor

D. The database fields should have been changed only during the annual PCI DSS assessment

ANSWER: B

Explanation:

Documentation must be updated as part of the change-control process. Changes to payment applications and associated data handling can affect PCI DSS scope, security controls, and the accuracy of evidence used during an assessment. Updating relevant documentation ensures that the entity maintains an accurate understanding of its environment and can evaluate the security impact of future changes.

Approval, testing, and back-out procedures are required change-control elements, but they do not replace the requirement to update applicable documentation. The change record should identify and update the affected data-flow and system documentation before or as part of implementation.

QUESTION NO: 3

If disk encryption is used to protect account data what requirement should be met for the disk encryption solution?

A. Access to the disk encryption must be managed independently of the operating system access control mechanisms

B. The disk encryption system must use the same user account authenticator as the operating system

C. The decryption keys must be associated with the local user account database

D. The decryption keys must be stored within the local user account database

ANSWER: A

Explanation:

Access to the disk encryption must be managed independently of the operating system access control mechanisms is correct. PCI DSS permits disk encryption to render stored PAN unreadable, but it requires a separation between access to the encrypted data and the operating system's native authentication and authorization controls. This separation ensures that a person who can authenticate to, administer, or compromise an operating-system account does not automatically gain the ability to decrypt or access cardholder data. In practice, the encryption solution should use controls that are distinct from the operating system's normal user-account and permission model, such as separately managed encryption credentials, keys, or authentication mechanisms. The goal is to preserve effective protection for account data even where operating-system access is obtained or altered. This requirement is specifically relevant to whole-disk or disk-level encryption, because those technologies can otherwise decrypt data transparently for an authenticated operating-system user. PCI DSS requirements for protecting stored account data and the applicable testing procedures are published in the PCI SSC PCI DSS document library. PCI SSC also provides supporting implementation guidance and FAQs through its official FAQ portal.

QUESTION NO: 4

An entity performs a quarterly walkthrough of each facility to look for unauthorized wireless access points. The personnel conducting the walkthrough do not use a wireless analyzer, and no wireless intrusion-detection or intrusion-prevention capability is deployed. Which statement is correct?

A. The process is sufficient because it is performed once each quarter

B. The process is sufficient if personnel document the areas inspected during each walkthrough

C. The process is not sufficient because it lacks an approved technical method for detecting unauthorized wireless access points

D. The process is required only where the entity provides authorized wireless access to cardholder data systems

ANSWER: C

Explanation:

The entity's process is not sufficient because visual walkthroughs alone may not detect unauthorized wireless access points. PCI DSS requires entities to identify and respond to unauthorized wireless access points using a wireless analyzer at least quarterly or by deploying a wireless intrusion-detection and/or intrusion-prevention mechanism.

An unauthorized device may be concealed, may not be physically apparent, or may be embedded in other equipment. The required detection method must therefore provide a technical means to identify wireless activity rather than relying only on physical inspection.

QUESTION NO: 5

Which scenario meets PCI DSS requirements for restricting access to databases containing cardholder data?

A. User access to the database is only through programmatic methods

B. User access to the database is restricted to system and network administrators

C. Application IDs for database applications can only be used by database administrators

D. Direct queries to the database are restricted to shared database administrator accounts

ANSWER: A

Explanation:

User access to the database is only through programmatic methods is the scenario that meets the database-access restriction. PCI DSS requires access to cardholder data and system components to be limited according to business need to know and least privilege. Routing a user's interaction through an authorized application or other programmatic mechanism supports that control because the mechanism can consistently authenticate the user, enforce the user's assigned authorization, limit available functions and queries, and generate auditable activity records. It also separates ordinary user activity from the database-management layer, reducing unnecessary exposure of stored cardholder data.

For database repositories that store cardholder data, access controls must be designed so that only the necessary users and processes can retrieve or query data required for their defined job responsibilities. A properly designed application path can apply these restrictions using distinct user identities, role-based permissions, secure session handling, and protected database credentials. The entity must still configure the application and database privileges according to least privilege and review access regularly; using a programmatic access path is not a substitute for those controls. PCI SSC's current standard and supporting materials are available through the PCI DSS standards page and the PCI SSC Document Library.

QUESTION NO: 6

What must the assessor verify when testing that PAN is protected whenever it is sent over the Internet?

A. The security protocol is configured to support earlier versions

B. The PAN is encrypted with strong cryptography

C. The security protocol is configured to accept all digital certificates

D. The PAN is securely deleted once the transmission has been sent

ANSWER: B

Explanation:

The PAN is encrypted with strong cryptography is correct because PCI DSS requires primary account number to be protected with strong cryptography whenever it is transmitted over open, public networks, including the Internet. During assessment procedures, the assessor examines the entity's documented transmission methods and configurations, then verifies that the cryptographic protection is actually in place for each applicable transmission channel. This includes confirming that the security protocol and cryptographic implementation protect PAN confidentiality in transit and are implemented according to industry best practices. The objective is to prevent an unauthorized party from reading PAN if network traffic is intercepted while traversing an untrusted network. "Strong cryptography" means cryptography based on accepted industry-tested algorithms and appropriate key strengths, with secure implementation and key management. PCI DSS also requires the use of secure protocols configured to support only secure versions and secure configurations, which helps ensure the encryption protecting PAN remains effective. The assessor should validate this through evidence such as network diagrams, configuration settings, protocol testing, and observations of transmission paths. See PCI DSS Requirement 4 and its testing procedures in the PCI DSS v4.0.1 standard, as well as PCI SSC's guidance on strong cryptography.

QUESTION NO: 7

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

A. Ensure all vulnerabilities are addressed within 30 days

B. Replace the need to quarterly ASV scans

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:

The correct answer is “Prioritize the highest risk items so they can be addressed more quickly.” PCI DSS requires entities to identify and address security vulnerabilities, including by assigning a risk ranking to newly discovered vulnerabilities. The purpose of that ranking is to give the entity a consistent, risk-based basis for determining remediation priority. Vulnerabilities that present greater potential impact to the security of the cardholder data environment—for example, based on severity, exploitability, exposure, affected systems, and available compensating protections—should receive attention ahead of lower-risk issues. This helps ensure remediation resources are directed first to the conditions that create the most significant security risk, while supporting timely patching and vulnerability management overall. PCI DSS does not prescribe one universal remediation timeframe solely from the act of assigning a ranking; rather, the entity’s documented process must define how risk rankings are used to prioritize and address vulnerabilities. This principle is reflected in PCI DSS Requirement 6.3.3, which requires security vulnerabilities to be identified, risk ranked, and addressed. See the PCI DSS document library and PCI SSC’s merchant guidance resources for official PCI DSS materials.