

PCI SSC

Assessor_New_V4

Assessor_New_V4 Exam



For More Information – Visit link below:

<https://www.examsboost.com/>

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

Which systems must have anti-malware solutions'

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

Answer: D

Explanation:

According to the PCI DSS v3.2.1 Quick Reference Guide 1 , any in-scope system except for those identified as not at risk from malware must have anti-malware solutions installed and configured according to best practices. This is one of the requirements for preventing malware infections that could compromise cardholder data.

Question: 2

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: C

Explanation:

According to the PCI DSS v3.2.1 Quick Reference Guide 1 , pre-production environments that are located within the cardholder data environment can be used for testing, as long as they are not accessible from untrusted networks and are monitored for any changes or vulnerabilities. This is one of the requirements for ensuring that testing environments are isolated from production environments.

Question: 3

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:

The PCI DSS requires that access to databases containing cardholder data is restricted to authorized users and applications, and that direct access to such databases is prohibited. According to the PCI DSS Requirement 7.1.2, "Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities." Furthermore, according to the PCI DSS Requirement 8.3.1, "Implement multi-factor authentication for all non-console access into the cardholder data environment for personnel with administrative access." Therefore, the scenario that meets the PCI DSS requirements for restricting access to databases containing cardholder data is the one where user access to the database is only through programmatic methods, such as through an application interface that enforces authentication, authorization, and encryption. The other scenarios either allow direct access to the database, or do not limit the access to the least privileges necessary, or do not use multi-factor authentication for administrative access. References : [PCI DSS v3.2.1], Card Production Security Assessor - Logical - Credly

Question: 4

An entity accepts e-commerce payment card transactions and stores account data in a database The database server and the web server are both accessible from the Internet The database server and the web server are on separate physical servers. What is required for the entity to meet PCI DSS requirements?

- A. The web server and the database server should be installed on the same physical server
- B. The database server should be relocated so that it is not accessible from untrusted networks
- C. The web server should be moved into the internal network
- D. The database server should be moved to a separate segment from the web server to allow for more concurrent connections

Answer: B

Explanation:

According to the PCI DSS v3.2.1 Quick Reference Guide 1 , the database server should be relocated so that it is not accessible from untrusted networks. This is one of the requirements for protecting cardholder data in transit and at rest.

Question: 5

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:

According to the PCI DSS v3.2.1 Quick Reference Guide 1 , the intent of assigning a risk ranking to vulnerabilities is to prioritize the highest risk items so they can be addressed more quickly, rather than ensuring all vulnerabilities are addressed within 30 days or replacing the need to quarterly ASV scans or ensuring that critical security patches are installed at least quarterly. This is one of the requirements for ensuring that vulnerabilities are identified and mitigated as soon as possible.

Thank You for Trying Our Product

For More Information – **Visit link below:**

<https://www.examsboost.com/>

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/assessor-new-v4>