PassTest

Bessere Qualität , bessere Dienstleistungen!

Q&A

http://www.passtest.de

Einjährige kostenlose Aktualisierung

Exam : **Assessor_New_V4**

Title : Assessor_New_V4 - Assessor_New_V4 Exam

Version : DEMO

1.In the ROC Repotting Template, which of the following is the best approach for a response where the requirement was in Place''?
A. Details of the entity s project plan for implementing the requirement
B. Details of how the assessor observed the entity s systems were compliant with the requirement
C. Details of the entity s reason for not implementing the requirement
D. Details of how the assessor observed the entity s systems were not compliant with the requirement
Answer: B
Explanation:
when a cryptographic key is retired and replaced with a new key, the assessor will verify that the assessor observed the entity's systems were compliant with the requirement, which means they should have implemented compensating controls to address any weaknesses or gaps in the customized control. This is one of the requirements for ensuring that an entity can use both approaches when appropriate.

2.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 requirements7
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 Guide1, 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.

3.An organization has implemented a change-detection mechanism on their systems.
How often must critical file comparisons be performed?
A. At least weekly
B. Periodically as defined by the entity
C. Only after a valid change is installed
D. At least monthly
Answer: A
Explanation:
PCI DSS Requirement 11.5 states that entities must deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly1. This is to ensure that any unauthorized or malicious changes to the files are detected and reported in a timely manner, and that the integrity and security of the files are maintained. Critical files are those that affect the security of the cardholder data environment (CDE), such as system files, application executables, configuration files, database files, and log files2. Therefore, the correct answer is option

4.Which statement is true regarding the use of intrusion detection techniques, such as intrusion detection systems and/or intrusion protection systems (IDS'IPS)?
A. Intrusion detection techniques are required on all system components
B. Intrusion detection techniques are required to alert personnel of suspected compromises
C. Intrusion detection techniques are required to isolate systems in the cardholder data environment from all other systems
D. Intrusion detection techniques are required to identify all instances of cardholder data
Answer: B
Explanation:
According to the PCI DSS v3.2.1 Quick Reference Guide1, intrusion detection techniques are required to alert personnel of suspected compromises that could compromise cardholder data or payment processing systems. This is one of the requirements for identifying and mitigating vulnerabilities that could compromise cardholder data.

5.Which of the following statements is true whenever a cryptographic key is retired and replaced with a new key?
A. The retired key must not be used for encryption operations
B. Cryptographic key components from the retired key must be retained for 3 months before disposal
C. A new key custodian must be assigned
D. All data encrypted under the retired key must be securely destroyed
Answer: A
Explanation:
PCI DSS Requirement 3.6.4 states that entities must retire or replace keys when the keys have reached the end of their cryptoperiod, which is the time span during which a specific key can be used for cryptographic operations1. The retired key must not be used for encryption operations, as it may have been compromised or weakened by cryptanalysis, and may not provide adequate protection for the data. A The retired key may still be used for decryption operations, if needed, to access historical data that was encrypted under the retired key2. Therefore, the correct answer is option A.
The other options are not true regarding the cryptographic key retirement and replacement. A Option B is not true because PCI DSS does not specify a retention period for the cryptographic key components from the retired key, although it requires entities to securely delete cryptographic material when it is no longer needed for business or legal reasons1.Â Option C is not true because PCI DSS does not require a new key custodian tobe assigned, although it requires entities to define and document the roles, responsibilities, and accountability of all key custodians1.Â Option D is not true because PCI DSS does not require all data encrypted under the retired key to be securely destroyed, although it requires entities to render cardholder data unreadable when it is no longer needed for business or legal reasons1. A
References:
PCI DSS v3.2.1
Cryptographic Key Blocks - PCI Security Standards Council