Boost up Your Certification Score

PCI SSC
ISA-N_Retake
PCI Internal Security Assessor Retake 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.

Visit us at: https://www.examsboost.com/test/isa-n-retake

Latest Version: 6.0

Question: 1

Which of the following parties is responsible for completion of the Controls Matrix for the Customized Approach?

A. Only a Qualified Security Assessor (QSA)
B. Either a QSA, AQSA, or PCIP.
C. Entity being assessed
D. Card brands or acquirer

Answer: C

Explanation:
According to the PCI DSS v3.2.1 Quick Reference Guide 1 , assigning a unique ID to each person is intended to ensure individual users are accountable for their own actions, rather than shared accounts or group accounts based on need-to-know. This is one of the requirements for ensuring that user accounts are properly managed and controlled.

Question: 2

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

Question: 3

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:
According to requirement 3.1.2, multi-tenant service providers must ensure that customers cannot access another entity's cardholder data environment, which means they should isolate each customer's cardholder data from other customers' cardholder data and prevent unauthorized access or disclosure. This is one of the requirements for ensuring that multi-tenant service providers protect each customer's cardholder data.

Question: 4

Which scenario meets PCI DSS requirements for critical systems to have correct and consistent time?

A. Each internal system is configured to be its own time server.
B. Access to time configuration settings is available to all users of the system.
C. Central time servers receive time signals from specific, approved external sources
D. Each internal system peers directory with an external source to ensure accuracy of time updates

Answer: C

Explanation:
critical systems must have correct and consistent time, which means they should use a reliable time source and synchronize their clocks with other systems. This is one of the requirements for ensuring that critical systems have accurate time.

Question: 5

Which of the following describes "stateful responses' to communication initiated by a trusted network?

A. Administrative access to respond to requests to change the firewall is limited to one individual at a time
B. Active network connections are tracked so that invalid response' traffic can be identified.
C. A current baseline of application configurations is maintained and any mis-configuration is responded to promptly
D. Logs of user activity on the firewall are correlated to identify and respond to suspicious behavior

Answer: B

Explanation:
According to the PCI DSS v3.2.1 Quick Reference Guide 1 , active network connections are tracked so that invalid response traffic can be identified. This is one of the requirements for preventing replay attacks and ensuring secure communication.

Question: 6

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

Answer: D

Explanation:
One of the best practices for hardening a firewall is to disable any firewall functions that are not needed in production, such as unused services, ports, protocols, or features. This reduces the attack surface and minimizes the potential for exploitation. According to the PCI Card Production Logical Security Requirements, section 3.2.1, “The firewall must be configured to deny all traffic by default and allow only traffic that is explicitly required for the card production environment.” Furthermore, section 3.2.2 states, “The firewall must be configured to block all unnecessary services, ports, protocols, and IP addresses.” References : PCI Card Production Logical Security Requirements , Card Production Security Assessor - Logical - Credly

Question: 7

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 ensuing 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: B

Explanation:
The customized approach is a new option in PCI DSS v4.0 that allows entities to use alternate security controls or new technologies that meet the PCI DSS Customized Approach Objective for a requirement 1 . The customized approach requires the entity to complete and document a Controls Matrix and a Targeted Risk Analysis (TRA) for each customized control, and to provide this documentation to the assessor 2 . The assessor’s role is to review the documentation, assess the customized control, and verify that the customized approach was correctly followed 3 . The assessor must also document the assessment of the customized control in the Report on Compliance (ROC), using the ROC Template provided by PCI SSC 4 . Therefore, the correct answer is option B.
The other options are not true regarding the role of the assessor in the customized approach. Option A is not true because the assessor does not need another assessor to verify the TRA, as the assessor is

responsible for reviewing and validating the TRA as part of the assessment process 3 . Option C is not true because the assessor can and must assess the control and the documentation, as well as document the work on the customized control in the ROC 3 4 . Option D is not true because the assessor is allowed to assist the entity with the completion of the Controls Matrix or the TRA, as long as the assessor does not design, develop, or implement the customized control for the entity 5 . References :
PCI DSS v4.0: Is the Customized Approach Right For Your Organization?
PCI DSS v4.0: Roles and Responsibilities for the Customized Approach
PCI DSS v4.0 Report on Compliance Template
PCI DSS v4.0
PCI DSS v4.0: Customized Approach Explained

Question: 8

Which of the following can be sampled for testing during a PCI DSS assessment?

A. PCI DSS requirements and testing procedures.
B. Compensating controls
C. Business facilities and system components
D. Security policies and procedures

Answer: C

Explanation:
According to the PCI DSS v3.2.1 Quick Reference Guide 1 , business facilities and system components can be sampled for testing during a PCI DSS assessment, as long as they are not critical components or components that are not in scope for testing. This is one of the requirements for ensuring that testing covers all relevant components and processes.

Question: 9

An LDAP server providing authentication services to the cardholder data environment is

A. in scope for PCI DSS.
B. not in scope for PCI DSS
C. in scope only if it stores processes or transmits cardholder data
D. in scope only if it provides authentication services to systems in the DMZ

Answer: A

Explanation:
An LDAP server is a type of directory service that provides authentication and authorization data to the cardholder data environment (CDE) 1 . According to the PCI DSS scoping and segmentation guidance 2 , any system that provides a security service to the CDE, such as authentication, is considered a connected or security-impacting system (Category 2) and is in scope for PCI DSS. This is because such systems can affect the security and controls of the CDE and the cardholder data (CHD) or sensitive authentication data (SAD) that it contains. Therefore, an LDAP server providing authentication services

to the CDE is in scope for PCI DSS, regardless of whether it stores, processes, or transmits CHD or SAD, or whether it provides authentication services to systems in the DMZ or not. References :
Guidance for PCI DSS Scoping and Network Segmentation
What Are the Effects of Using Active Directory as a Shared Service on PCI Compliance?
The Ultimate Guide To PCI DSS Scoping and Segmentation
LDAP - PCI Security Standards Council

Question: 10

Which of the following statements is true regarding track equivalent data on the chip of a payment card?

A. It is allowed to be stored by merchants after authorization if encrypted
B. It is sensitive authentication data
C. It is out of scope for PCI DSS
D. It is not applicable for PCI DSS Requirement 3.2

Answer: B

Explanation:
According to the PCI DSS v3.2.1 Quick Reference Guide 1 , track equivalent data on the chip of a payment card is sensitive authentication data, which means it can be used to authenticate a cardholder or a transaction, but it should not be stored or transmitted by merchants after authorization if encrypted. This is one of the requirements for preventing unauthorized access to sensitive authentication data.

Visit us at: https://www.examsboost.com/test/isa-n-retake

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

