IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **QSA_New_V4**

Title : Qualified Security Assessor V4 Exam

Version : DEMO

1.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
Explanation:
Comprehensive Detailed Step by Step Explanation with All PCI DSS and Qualified Security Assessor V4 References
Relevant PCI DSS Requirement: Internal vulnerability scans are discussed under PCI DSS Requirement 11.3.1, which requires organizations to perform internal vulnerability scanning as part of their regular vulnerability management process.
Frequency and Trigger for Internal Scans:
PCI DSS v4.0 explicitly states that internal vulnerability scans should be conducted at least quarterly and after any significant change.
A "significant change" can include modifications such as infrastructure upgrades, addition of new systems or software, and configuration changes that may impact security. Approved Scanning Vendor (ASV):
Internal scans do not require an Approved Scanning Vendor (ASV). ASVs are specifically used for external vulnerability scans.
Qualified Security Assessor (QSA) Involvement:
QSAs are not mandated to perform internal scans. Organizations can use internal teams or trusted third-party resources for this purpose, provided the scans meet PCI DSS criteria. Annual Scanning Misconception:
While annual compliance reports may include details of scanning activities, the requirement for internal scans is at least quarterly and event-triggered, not annually. Reference Verification:
Requirement 11.3.1 (PCI DSS v4.0): Clearly outlines the need for quarterly scans and post-significant-change scans.
ROC and SAQ Templates: Reinforce the requirement that scans are both regular and reactive to environmental changes.

2.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 ensuring 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:

Customized Approach Overview:
Under PCI DSS v4.0, entities can use a Customized Approach to meet requirements by implementing controls tailored to their environment. This allows flexibility while still achieving the intent of the security requirement.
Role of Assessors:
Assessors (QSAs) are responsible for evaluating both the implementation of customized controls and ensuring these controls fulfill the security objectives of the PCI DSS requirements.
QSAs must document the evaluation, evidence reviewed, and results in the Report on Compliance (ROC).
Controls Matrix and Targeted Risk Analysis (TRA):
The Controls Matrix and TRA are key components of the Customized Approach. QSAs assist in verifying the accuracy and completeness of these tools during assessments. Documenting in the ROC:
The ROC must include a narrative explaining the assessor's findings regarding the customized control, validation methods, and any evidence collected.
Relevant PCI DSS v4.0 Guidance:
Appendix D and E of the PCI DSS v4.0 ROC Template emphasize that QSAs can evaluate and confirm adherence to the Customized Approach provided this is documented comprehensively in the ROC.

3.Security policies and operational procedures should be?
A. Encrypted with strong cryptography.
B. Stored securely so that only management has access.
C. Reviewed and updated at least quarterly.
D. Distributed to and understood by ail affected parties.
Answer: D
Explanation:
Requirement Context:
PCI DSS Requirement 12.5 mandates that security policies and operational procedures are not only documented but also distributed to relevant parties to ensure clarity and compliance. Importance of Distribution and Awareness:
All affected parties, including employees, contractors, and third parties with access to the cardholder data environment (CDE), must receive and understand the policies. This ensures they adhere to the security measures.
Review and Updates:
Security policies must be kept up to date and reviewed at least annually or after significant changes in the environment. While other options such as encryption or restricted access are important for security, the critical focus is on distribution and awareness to ensure operational effectiveness. Testing and Validation:
During assessments, QSAs validate the implementation by examining training records, communication logs, and acknowledgment forms signed by affected parties. Relevant PCI DSS v4.0 Guidance:
Section 12.5.1 of PCI DSS v4.0 outlines that the dissemination of policies must ensure that all personnel understand their roles in securing the environment.

4.Which of the following is true regarding compensating controls?
A. A compensating control is not necessary if all other PCI DSS requirements are in place.

B. A compensating control must address the risk associated with not adhering to the PCI DSS requirement.
C. An existing PCI DSS requirement can be used as compensating control if it is already implemented.
D. A compensating control worksheet is not required if the acquirer approves the compensating control.
Answer: B
Explanation:
Compensating Controls Definition and Purpose
A compensating control is an alternate measure that satisfies the intent of a specific PCI DSS requirement and provides an equivalent level of security.
The rationale and risk mitigation must be explicitly documented using the Compensating Control Worksheet (CCW).
Mandatory Documentation
PCI DSS v4.0 mandates the use of a CCW when implementing compensating controls. This applies regardless of acquirer approvals.
The CCW requires detailed documentation including:
Constraints preventing the original requirement from being implemented.
Justification for the compensating control.
Description of the control and evidence of its effectiveness.
Using Existing Requirements
If an existing PCI DSS requirement (e.g., Requirement 5 for antivirus) is already implemented and can mitigate the risks of not meeting another requirement, it may qualify as a compensating control.
Approval and Review Process
QSAs must validate the implementation, effectiveness, and appropriateness of compensating controls during the assessment process

5.Where an entity under assessment is using the customized approach, which of the following steps is the responsibility of the assessor?
A. Monitor the control.
B. Derive testing procedures and document them in Appendix E of the ROC.
C. Document and maintain evidence about each customized control as defined in Appendix E of PCI DSS.
D. Perform the targeted risk analysis as per PCI DSS requirement 12.3.2.
Answer: C
Explanation:
Customized Approach Overview
Appendix E of PCI DSS v4.0 outlines the customized approach, which allows entities to demonstrate their control effectiveness using methods that differ from the defined approach.
Assessor Responsibilities QSAs must document and maintain detailed evidence for each customized control implemented by the entity.
Evidence must support how the customized control meets the security objectives of the original requirement.
Testing and Validation
The QSA must perform validation to confirm the customized control’s adequacy and effectiveness and ensure it sufficiently addresses the requirement’s intent. Documentation

All findings, testing procedures, and conclusions must be recorded in the Report on Compliance (ROC) Appendix E, providing traceability and transparency.