Payment Card Industry
Data Security Standard

PCI DSS v4.0.1 Supplemental Report on Compliance Template

Designated Entities Supplemental Validation

August 2024

Document Changes

Date	Version	Description
June 2015	For use with PCI DSS v3.1 Revision 1.0	To introduce the template for submitting Supplemental Reports on Compliance for Designated Entities. *This document is intended for use with version 1.0 of the PCI DSS Designated Entities Supplemental Validation.*
May 2016	For use with PCI DSS v3.2 Revision 1.0	To update the template to align with PCI DSS v3.2.
December 2018	For use with PCI DSS v3.2.1 Revision 1.0	To update the template to align with PCI DSS v3.2.1.
June 2022	For use with PCI DSS v4.0	To update the template to align with PCI DSS v4.0.
December 2022	For use with PCI DSS v4.0 Revision 1	Updated to remove In Place with Remediation as a reporting option.
July 2024	For use with PCI DSS v4.0.1	To update the template to align with PCI DSS v4.0.1 and with updated formatting in the ROC Template for v4.0.1.

Introduction to the PCI DSS v4.0.1 Supplemental Report on Compliance (ROC) Template for Designated Entities Supplemental Validation

Instructions for Submission

This document, the *PCI DSS v4.0.1 Supplemental Report on Compliance Template - Designated Entities Supplemental Validation* ("Supplemental ROC Template" or "S-ROC"), is the mandatory template for Qualified Security Assessors (QSAs) completing an assessment of a designated entity against the *PCI DSS v4.0.1 Appendix A3: Designated Entities Supplemental Validation.*

Note that an entity is *ONLY* required to undergo an assessment according to this document if instructed to do so by an acquirer or a payment brand.

This "Supplemental ROC Template" or "S-ROC" is to be completed according to the same instructions provided in the *PCI DSS v4.0.1 Report on Compliance (ROC) Template*. Refer to the *PCI DSS v4.0.1 ROC Template* and the *PCI DSS v4.x Report on Compliance Template – Frequently Asked Questions* documents on the PCI SSC website for detailed instructions on how to complete these reporting templates. Do not delete any content from any place in this document, including this section and the versioning above. Excessive personalization and changes to sections – including additional sections - may not be accepted by accepting entities, and personalization should be limited to the title page.

The S-ROC template is an addendum to the ROC Template and is not intended to stand alone. Because of this, details related to Scope of Work, Details of Reviewed Environment, Remote Assessment Activities, etc. that are applicable to the environment reviewed for the S-ROC must be included in the applicable sections in the full ROC for that entity. For example, the list of evidence in the full ROC must also include any evidence reviewed during assessment of activities for the *PCI DSS v4.0.1 Appendix A3: Designated Entities Supplemental Validation*.

While this supplemental validation would typically be done in conjunction with a full PCI DSS assessment, entities should contact their payment brand and/or acquirer with any questions about completing and submitting these reports.

The Customized Approach is not an option Designated Entities Supplemental Validation and reporting for it is not included in this supplemental ROC template.

Note that an entity is *ONLY* required to undergo an assessment according to this document if instructed to do so by an acquirer or a payment brand.

Addendum to PCI DSS v4.0.1 ROC Template for Appendix A3: Designated Entities Supplemental Validation (DESV)

1 Summary of DESV Results

Indicate all the findings and whether compensating controls were used within each DESV requirement. Select all that apply. For example, ***In Place*** and ***Not Applicable*** must both be selected for Requirement A3.1 if there is at least one sub-requirement marked ***In Place*** and one sub-requirement marked ***Not Applicable***. The column for Compensating Controls must be selected if there is at least one sub-requirement within the DESV requirements that used a compensating control.

DESV Requirement	Assessment Finding Select all options that apply.			Select Below If Compensating Control Was Used
	In Place	Not Applicable	Not in Place	
Requirement A3.1:	□	□	□	□
Requirement A3.2:	□	□	□	□
Requirement A3.3:	□	□	□	□
Requirement A3.4:	□	□	□	□
Requirement A3.5:	□	□	□	□

In the sections below, identify the DESV requirements with the following results and assessment method. If there are none, enter “Not Applicable.”

Note: *Natural grouping of requirements is allowed (for example, Req. A3.1.1, A3.1.2, A3.1.3, or A3.1.1 through A3.1.4, etc.) to reduce the number of individual requirements listed.*

Not Applicable	Not in Place Due to a Legal Restriction	Not in Place Not Due to a Legal Restriction	Compensating Control

2 Findings and Observations

Requirement Description
A3.1 A PCI DSS compliance program is implemented.

PCI DSS Requirement
A3.1.1 Responsibility is established by executive management for the protection of account data and a PCI DSS compliance program that includes: • Overall accountability for maintaining PCI DSS compliance. • Defining a charter for a PCI DSS compliance program. • Providing updates to executive management and board of directors on PCI DSS compliance initiatives and issues, including remediation activities, at least once every 12 months. **PCI DSS Reference**: *Requirement 12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach*** *Appendix C to support this method.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.1.1.a Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **documentation** examined for this testing procedure.	
A3.1.1.b Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for the **company's PCI DSS charter** examined for this testing procedure.	
A3.1.1.c Examine executive management and board of directors	**Identify** the evidence reference number(s) from *Section 6 of the ROC*	

meeting minutes and/or presentations to ensure PCI DSS compliance initiatives and remediation activities are communicated at least once every 12 months.	*Template* for all **executive management and board of directors meeting minutes and/or presentations** examined for this testing procedure.	

PCI DSS Requirement
A3.1.2 A formal PCI DSS compliance program is in place that includes: • Definition of activities for maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities. • Annual PCI DSS assessment processes. • Processes for the continuous validation of PCI DSS requirements (for example, daily, weekly, every three months, as applicable per the requirement). • A process for performing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions. **PCI DSS Reference:** *Requirements 1-12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.1.2.a Examine information security policies and procedures to verify that processes are defined for a formal PCI DSS compliance program that includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **information security policies and procedures** examined for this testing procedure.	
A3.1.2.b Interview personnel and observe compliance activities to verify that a formal PCI DSS compliance program is implemented in	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	

accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **observations of compliance activities** for this testing procedure.	

PCI DSS Requirement
A3.1.3 PCI DSS compliance roles and responsibilities are specifically defined and formally assigned to one or more personnel, including: • Managing PCI DSS business-as-usual activities. • Managing annual PCI DSS assessments. • Managing continuous validation of PCI DSS requirements (for example, daily, weekly, every three months, as applicable per the requirement). • Managing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions. **PCI DSS Reference**: *Requirement 12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ***Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.1.3.a Examine information security policies and procedures and interview personnel to verify that PCI DSS compliance roles and responsibilities are specifically defined and formally assigned to one or more personnel in accordance with all elements of this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **information security policies and procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	
A3.1.3.b Interview responsible personnel and verify they are familiar with and performing their designated PCI DSS compliance responsibilities.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
A3.1.4 Up-to-date PCI DSS and/or information security training is provided at least once every 12 months to personnel with PCI DSS compliance responsibilities (as identified in A3.1.3). **PCI DSS Reference:** *Requirement 12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.1.4.a Examine information security policies and procedures to verify that PCI DSS and/or information security training is required at least once every 12 months for each role with PCI DSS compliance responsibilities.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **information security policies and procedures** examined for this testing procedure.	
A3.1.4.b Interview personnel and examine certificates of attendance or other records to verify that personnel with PCI DSS compliance responsibility receive up-to-date PCI DSS and/or similar information security training at least once every 12 months.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **certificates of attendance or other records** examined for this testing procedure.	

Requirement Description
A3.2 PCI DSS scope is documented and validated.

PCI DSS Requirement

A3.2.1 PCI DSS scope is documented and confirmed for accuracy at least once every three months and upon significant changes to the in-scope environment. At a minimum, the scoping validation includes:

- Identifying all data flows for the various payment stages (for example, authorization, capture, settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce).
- Updating all data-flow diagrams per Requirement 1.2.4.
- Identifying all locations where account data is stored, processed, and transmitted, including but not limited to 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups.
- For any account data found outside of the currently defined CDE, either 1) securely delete it, 2) migrate it into the currently defined CDE, or 3) expand the currently defined CDE to include it.
- Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE.
- Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.
- Identifying all connections to third-party entities with access to the CDE.
- Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.

PCI DSS Reference: *Scope of PCI DSS Requirements, Requirement 12.*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the “Required Reporting” column of the table in Assessment Findings in the ROC Template Instructions.* ***Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.2.1.a Examine documented results of scope reviews and interview personnel to verify that the reviews are performed: • At least once every three months. • After significant changes to the in-scope environment.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	
A3.2.1.b Examine documented results of scope reviews occurring at least once every three months to verify that scoping validation includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **documented results of scope reviews** examined for this testing procedure.	

PCI DSS Requirement
A3.2.2 PCI DSS scope impact for all changes to systems or networks is determined, including additions of new systems and new network connections. Processes include: • Performing a formal PCI DSS impact assessment. • Identifying applicable PCI DSS requirements to the system or network. • Updating PCI DSS scope as appropriate. • Documented sign-off of the results of the impact assessment by responsible personnel (as defined in A3.1.3). **PCI DSS Reference:** *Scope of PCI DSS Requirements; Requirements 1-12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in* Assessment Findings *in the ROC Template Instructions.* ****Complete and attach*** *Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.2.2 Examine change documentation and interview personnel to verify that for each change to systems or networks the PCI DSS scope impact is determined, and includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **change documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
A3.2.2.1 Upon completion of a change, all relevant PCI DSS requirements are confirmed to be implemented on all new or changed systems and networks, and documentation is updated as applicable. **PCI DSS Reference:** *Scope of PCI DSS Requirements; Requirement 1-12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ***Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.2.2.1 Examine change records and the affected systems/networks, and interview personnel to verify that all relevant PCI DSS requirements were confirmed to be implemented and documentation updated as part of the change.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **change records** examined for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **affected systems/networks** examined for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
A3.2.3 Changes to organizational structure result in a formal (internal) review of the impact to PCI DSS scope and applicability of controls. **PCI DSS Reference:** *Requirement 12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.2.3 Examine policies and procedures to verify that a change to organizational structure results in formal a review of the impact on PCI DSS scope and applicability of controls.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **policies and procedures** examined for this testing procedure.	

PCI DSS Requirement
A3.2.4 If segmentation is used, PCI DSS scope is confirmed as follows: - Per the entity's methodology defined at Requirement 11.4.1. - Penetration testing is performed on segmentation controls at least once every six months and after any changes to segmentation controls/methods. - The penetration testing covers all segmentation controls/methods in use. - The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. **PCI DSS Reference:** *Requirement 11*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response	
A3.2.4 Examine the results from the most recent penetration test to verify that the test was conducted in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for the **results from the most recent penetration test** examined for this testing procedure.		

PCI DSS Requirement
A3.2.5 A data-discovery methodology is implemented that: • Confirms PCI DSS scope. • Locates all sources and locations of cleartext PAN at least once every three months and upon significant changes to the CDE or processes. • Addresses the potential for cleartext PAN to reside on systems and networks outside the currently defined CDE. **PCI DSS Reference**: *Scope of PCI DSS Requirements*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.2.5.a Examine the documented data-discovery methodology to verify it includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for the **documented data-discovery methodology** examined for this testing procedure.	
A3.2.5.b Examine results from recent data discovery efforts, and interview responsible personnel to verify that data discovery is performed at least once every three months and upon significant changes to the CDE or processes.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **results from recent data discovery efforts** examined for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
A3.2.5.1 Data discovery methods are confirmed as follows: • Effectiveness of methods is tested. • Methods are able to discover cleartext PAN on all types of system components and file formats in use. • The effectiveness of data-discovery methods is confirmed at least once every 12 months. **PCI DSS Reference:** *Scope of PCI DSS Requirements*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	**Not Applicable**	**Not in Place**	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ***Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.2.5.1.a Interview personnel and review documentation to verify: • The entity has a process in place to test the effectiveness of methods used for data discovery. • The process includes verifying the methods are able to discover cleartext PAN on all types of system components and file formats in use.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **documentation** examined for this testing procedure.	
A3.2.5.1.b Examine the results of effectiveness tests to verify that the effectiveness of data-discovery methods is confirmed at least once every 12 months.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for the **results of effectiveness tests** examined for this testing procedure.	

PCI DSS Requirement
A3.2.5.2 Response procedures are implemented to be initiated upon the detection of cleartext PAN outside the CDE to include: Determining what to do if cleartext PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Determining how the data ended up outside the CDE. • Remediating data leaks or process gaps that resulted in the data being outside the CDE. • Identifying the source of the data. • Identifying whether any track data is stored with the PANs.

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the “Required Reporting” column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor’s Response
A3.2.5.2.a Examine documented response procedures to verify that procedures for responding to the detection of cleartext PAN outside the CDE are defined and include all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **documented response procedures** examined for this testing procedure.	
A3.2.5.2.b Interview personnel and examine records of response actions to verify that remediation activities are performed when cleartext PAN is detected outside the CDE.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	

	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **records of response actions** examined for this testing procedure.	

PCI DSS Requirement
A3.2.6 Mechanisms are implemented for detecting and preventing cleartext PAN from leaving the CDE via an unauthorized channel, method, or process, including mechanisms that are: • Actively running. • Configured to detect and prevent cleartext PAN leaving the CDE via an unauthorized channel, method, or process. • Generating audit logs and alerts upon detection of cleartext PAN leaving the CDE via an unauthorized channel, method, or process. **PCI DSS Reference:** *Scope of PCI DSS Requirements, Requirement 12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ***Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.2.6.a Examine documentation and observe implemented mechanisms to verify that the mechanisms are in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **observations of the implemented mechanisms** for this testing procedure.	
A3.2.6.b Examine audit logs and alerts, and interview responsible personnel to verify that alerts are investigated.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **audit logs and alerts** examined for this testing procedure.	

	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
A3.2.6.1 Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include: • Procedures for the prompt investigation of alerts by responsible personnel. • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss. **PCI DSS Reference:** *Requirement 12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	**Not Applicable**	**Not in Place**	
□	□	□	□
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.2.6.1.a Examine documented response procedures to verify that procedures for responding to the attempted removal of cleartext PAN from the CDE via an unauthorized channel, method, or process include all elements specified in this requirement: • Procedures for the prompt investigation of alerts by responsible personnel. • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **documented response procedures** examined for this testing procedure.	
A3.2.6.1.b Interview personnel and examine records of actions taken when cleartext PAN is detected leaving the CDE via an unauthorized channel, method, or process and	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	

verify that remediation activities were performed.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **records of actions taken** examined for this testing procedure.	

Requirement Description
A3.3 PCI DSS is incorporated into business-as-usual (BAU) activities.

PCI DSS Requirement

A3.3.1 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of:

- Network security controls
- IDS/IPS
- FIM
- Anti-malware solutions
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation controls (if used)
- Automated audit log review mechanisms. *This bullet is a* ***best practice*** *until* ***31 March 2025****, after which they will be required as part of Requirement A3.3.1 and must be fully considered during a PCI DSS assessment.*
- Automated code review tools (if used). *This bullet is a* ***best practice*** *until* ***31 March 2025****, after which they will be required as part of Requirement A3.3.1 and must be fully considered during a PCI DSS assessment.*

PCI DSS Reference: *Requirements 1-12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	**Not Applicable**	**Not in Place**	
□	□	□	□
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor’s Response
A3.3.1.a Examine documented policies and procedures to verify that processes are defined to promptly detect, alert, and address critical security control failures in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **documented policies and procedures** examined for this testing procedure.	
A3.3.1.b Examine detection and alerting processes, and interview personnel to verify that processes are implemented for all critical security controls specified in this requirement and that each failure of a critical security control results in the generation of an alert.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **detection and alerting processes** examined for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
A3.3.1.1 Failures of any critical security control systems are responded to promptly. Processes for responding to failures in security control systems include: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure, including root cause, and documenting remediation required to address the root cause. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls. **PCI DSS Reference:** *Requirements 1-12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the “Required Reporting” column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor’s Response
A3.3.1.1.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond promptly to a security control failure in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **documented policies and procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	

A3.3.1.1.b Examine records to verify that security control failures are documented to include: • Identification of cause(s) of the failure, including root cause. • Duration (date and time start and end) of the security failure. • Details of the remediation required to address the root cause.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **records** examined for this testing procedure.	

PCI DSS Requirement
A3.3.2 Hardware and software technologies are reviewed at least once every 12 months to confirm whether they continue to meet the organization's PCI DSS requirements. **PCI DSS Reference:** *Requirements 2, 6, 12.*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.3.2.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to review hardware and software technologies to confirm whether they continue to meet the organization's PCI DSS requirements.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **documented policies and procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	
A3.3.2.b Review the results of the recent reviews of hardware and software technologies to verify reviews are performed at least once every 12 months.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for the **results of the recent reviews** examined for this testing procedure.	
A3.3.2.c Review documentation to verify that, for any technologies that have been determined to no longer meet the organization's PCI DSS requirements, a plan is in place to remediate the technology.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **documentation** examined for this testing procedure.	

PCI DSS Requirement
A3.3.3 Reviews are performed at least once every three months to verify BAU activities are being followed. Reviews are performed by personnel assigned to the PCI DSS compliance program (as identified in A3.1.3), and include: • Confirmation that all BAU activities, including A3.2.2, A3.2.6, and A3.3.1, are being performed. • Confirmation that personnel are following security policies and operational procedures (for example, daily log reviews, ruleset reviews for network security controls, and configuration standards for new systems). • Documenting how the reviews were completed, including how all BAU activities were verified as being in place. • Collection of documented evidence as required for the annual PCI DSS assessment. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program, as identified in A3.1.3. • Retention of records and documentation for at least 12 months, covering all BAU activities. **PCI DSS Reference**: *Requirements 1-12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.3.3.a Examine policies and procedures to verify that processes are defined for reviewing and verifying BAU activities in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **policies and procedures** examined for this testing procedure.	
A3.3.3.b Interview responsible personnel and examine records of reviews to verify that:	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	

- Reviews are performed by personnel assigned to the PCI DSS compliance program. - Reviews are performed at least once every three months.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **records of reviews** examined for this testing procedure.	

Requirement Description
A3.4 Logical access to the cardholder data environment is controlled and managed.
PCI DSS Requirement
A3.4.1 User accounts and access privileges to in-scope system components are reviewed at least once every six months to ensure user accounts and access privileges remain appropriate based on job function, and that all access is authorized. **PCI DSS Reference:** *Requirement 7*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	**Not Applicable**	**Not in Place**	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.4.1 Interview responsible personnel and examine supporting documentation to verify that: • User accounts and access privileges are reviewed at least every six months. • Reviews confirm that access is appropriate based on job function and that all access is authorized.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **documentation** examined for this testing procedure.	

Requirement Description
A3.5 Suspicious events are identified and responded to.

PCI DSS Requirement
A3.5.1 A methodology is implemented for the prompt identification of attack patterns and undesirable behavior across systems that includes: • Identification of anomalies or suspicious activity as it occurs. • Issuance of prompt alerts upon detection of suspicious activity or anomaly to responsible personnel. • Response to alerts in accordance with documented response procedures. **PCI DSS Reference:** *Requirements 10, 12*

Assessment Findings (select one)			Select If a Compensating Control Was Used*
In Place	Not Applicable	Not in Place	
□	□	□	□
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ****Complete and attach** Appendix C to support this method.*			

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A3.5.1.a Examine documentation and interview personnel to verify a methodology is defined and implemented to identify attack patterns and undesirable behavior across systems in a prompt manner, and includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	
A3.5.1.b Examine incident response procedures and interview responsible personnel to verify that:	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **incident response procedures** examined for this testing procedure.	

- On-call personnel receive prompt alerts. - Alerts are responded to per documented response procedures.	**Identify** the evidence reference number(s) from *Section 6 of the ROC Template* for all **interviews** conducted for this testing procedure.	