Payment Card Industry (PCI)
Data Security Standard

Supplemental Report on Compliance – Designated Entities

Reporting Template for use with PCI DSS v3.2
Appendix A3: Designated Entities Supplemental Validation

Revision 1.0

May 2016

Document Changes

Date	Version	Description
June 2015	For use with PCI DSS v3.1 Revision1.0	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

Introduction to the Supplemental ROC Template for PCI DSS v3.2, Appendix A3: Designated Entities Supplemental Validation

Instructions for Submission

This document, the *Reporting Template for use with PCI DSS v3.2, Appendix A3: Designated Entities Supplemental Validation, Revision 1.0* ("Supplemental ROC Template" or "S-ROC"), is the mandatory template for Qualified Security Assessors (QSAs) completing assessment of a designated entity against the *PCI DSS v3.2 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" document is to be completed according to the same instructions provided in the Reporting Template for PCI DSS v3.2. Refer to the *Reporting Template(s) for use with PCI DSS v3.2* and the *ROC Reporting Template for PCI DSS v3.x: Frequently Asked Questions (FAQs)* documents on the PCI SSC website for detailed instruction on how to complete these reporting templates. As such, 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 Reporting Template and is not intended to stand alone. Because of this, details related to Scope of Work, Details of Reviewed Environment and so on 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 interviewees in the full ROC should also include any persons interviewed during assessment of the *PCI DSS v3.2 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.

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 ROC Reporting Template - Reporting Template for use with PCI DSS v3.2, Appendix A3: Designated Entities Supplemental Validation

Findings and Observations

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.1 Implement a PCI DSS compliance program						
A3.1.1 Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program • Provide updates to executive management and board of directors on PCI DSS compliance initiatives and issues, including remediation activities, at least annually. ***PCI DSS Reference:*** *Requirement 12*			☐	☐	☐	☐
A3.1.1.a Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance.	**Identify the document(s) examined** to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance.	*<Report Findings Here>*				
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 company's PCI DSS charter document(s) examined** to verify the charter outlines the conditions under which the PCI DSS compliance program is organized.	*<Report Findings Here>*				
A3.1.1.c Examine executive management and board of directors meeting minutes and/or presentations to ensure PCI DSS compliance initiatives and remediation activities are communicated at least annually.	**Identify the sample of executive management and board of directors meeting minutes and/or presentations examined** to ensure PCI DSS compliance initiatives and remediation activities are communicated at least annually.	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.1.2 A formal PCI DSS compliance program must be in place to include: • 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, quarterly, etc. as applicable per requirement). • A process for performing business impact analyses to determine potential PCI DSS impacts for strategic business decisions ***PCI DSS Reference:*** *Requirements 1-12*			☐	☐	☐	☐
A3.1.2.a Examine information security policies and procedures to verify that processes are specifically defined for the following: • Maintaining and monitoring overall PCI DSS compliance, including business as usual activities • Annual PCI DSS assessment(s) • Continuous validation of PCI DSS requirements • Business impact analyses to determine potential PCI DSS impacts for strategic business decisions	**Identify the information security policies and procedures document(s) examined** to verify that processes are specifically defined for the following: • Maintaining and monitoring overall PCI DSS compliance, including business as usual activities • Annual PCI DSS assessment(s) • Continuous validation of PCI DSS requirements • Business impact analyses to determine potential PCI DSS impacts for strategic business decisions	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.1.2.b Interview personnel and observe compliance activities to verify that the defined processes are implemented for the following: • Maintaining and monitoring overall PCI DSS compliance, including business as usual activities • Annual PCI DSS assessment(s) • Continuous validation of PCI DSS requirements • Business impact analyses to determine potential PCI DSS impacts for strategic business decisions	**Identify the personnel interviewed** who confirm that defined processes are implemented for: • Maintaining and monitoring overall PCI DSS compliance, including business as usual activities • Annual PCI DSS assessment(s) • Continuous validation of PCI DSS requirements • Business impact analyses to determine potential PCI DSS impacts for strategic business decisions	*<Report Findings Here>*				
	Describe how compliance activities were observed to verify that defined processes are implemented for the following:					
	▪ Maintaining and monitoring overall PCI DSS compliance, including business as usual activities	*<Report Findings Here>*				
	▪ Annual PCI DSS assessment(s)	*<Report Findings Here>*				
	▪ Continuous validation of PCI DSS requirements	*<Report Findings Here>*				
	▪ Business impact analyses to determine potential PCI DSS impacts for strategic business decisions	*<Report Findings Here>*				
A3.1.3 PCI DSS compliance roles and responsibilities must be specifically defined and formally assigned to one or more personnel, including at least the following: • Managing PCI DSS business as usual activities • Managing annual PCI DSS assessments • Managing continuous validation of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement) • Managing business impact analyses to determine potential PCI DSS impacts for strategic business decisions ***PCI DSS Reference:*** *Requirement 12*			☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.1.3.a Examine information security policies and procedures and interview personnel to verify that roles and responsibilities are clearly defined and that duties are assigned to include at least the following: • Managing PCI DSS business as usual activities • Managing annual PCI DSS assessments • Managing continuous validation of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement) • Managing business impact analyses to determine potential PCI DSS impacts for strategic business decisions	**Identify the information security policies and procedures document(s) examined** to verify that roles and responsibilities are clearly defined and that duties are assigned to include at least the following: • Managing PCI DSS business as usual activities • Managing annual PCI DSS assessments • Managing continuous validation of PCI DSS requirements ▪ Managing business impact analyses to determine potential PCI DSS impacts for strategic business decisions	*<Report Findings Here>*				
	Identify the personnel interviewed who confirm that roles and responsibilities are clearly defined and that duties are assigned to include at least the following: • Managing PCI DSS business as usual activities • Managing annual PCI DSS assessments • Managing continuous validation of PCI DSS requirements ▪ Managing business impact analyses to determine potential PCI DSS impacts for strategic business decisions	*<Report Findings Here>*				
A3.1.3.b Interview responsible personnel and verify they are familiar with and performing their designated PCI DSS compliance responsibilities.	**Identify the personnel interviewed** who confirm that they are familiar with and performing their designated PCI DSS compliance responsibilities.	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.1.4 Provide up-to-date PCI DSS and/or information security training at least annually to personnel with PCI DSS compliance responsibilities (as identified in A3.1.3). ***PCI DSS Reference:*** *Requirement 12*			☐	☐	☐	☐
A3.1.4.a Examine information security policies and procedures to verify that PCI DSS and/or similar information security training is required at least annually for each role with PCI DSS compliance responsibilities.	**Identify the information security policies and procedures document(s) examined** to verify that PCI DSS and/or similar information security training is required at least annually for each role with PCI DSS compliance responsibilities.	*<Report Findings Here>*				
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 annually.	**Identify the personnel interviewed** who confirm that personnel with PCI DSS compliance responsibility receive up-to-date PCI DSS and/or similar information security training at least annually.	*<Report Findings Here>*				
	Identify the certificates of attendance or other records examined to verify that personnel with PCI DSS compliance responsibility receive up-to-date PCI DSS and/or similar information security training at least annually.	*<Report Findings Here>*				
A3.2 Document and validate PCI DSS scope						
A3.2.1 Document and confirm the accuracy of PCI DSS scope at least quarterly and upon significant changes to the in-scope environment. At a minimum, the quarterly scoping validation should include: • Identifying all in-scope networks and system components • Identifying all out-of-scope networks and justification for networks being out of scope, including descriptions of all segmentation controls implemented • Identifying all connected entities (e.g. third party entities with access to the cardholder data environment (CDE)) ***PCI DSS Reference:*** *Scope of PCI DSS Requirements*			☐	☐	☐	☐
A3.2.1.a Examine documented results of scope reviews and interview personnel to verify that the reviews are performed: • At least quarterly	**Identify the documented results of scope reviews examined** to verify that the reviews are performed: • At least quarterly • After significant changes to the in-scope environment	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
• After significant changes to the in-scope environment	**Identify the personnel interviewed** who confirm that the reviews are performed: • At least quarterly • After significant changes to the in-scope environment	*<Report Findings Here>*				
A3.2.1.b Examine documented results of quarterly scope reviews to verify the following is performed: • Identification of all in-scope networks and system components • Identification of all out-of-scope networks and justification for networks being out of scope, including descriptions of all segmentation controls implemented • Identification of all connected entities (e.g. third party entities with access to the CDE)	*Using the documented results of quarterly scope review identified at DE 2.1.a,* **describe how the documented results of quarterly scope reviews were observed** to verify that the following is performed:					
	• Identification of all in-scope networks and system components	*<Report Findings Here>*				
	• Identification of all out-of-scope networks and justification for networks being out of scope, including descriptions of all segmentation controls implemented	*<Report Findings Here>*				
	• Identification of all connected entities	*<Report Findings Here>*				
A3.2.2 Determine PCI DSS scope impact for all changes to systems or networks, including additions of new systems and new network connections. Processes must 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*			☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.2.2 Examine change documentation and interview personnel to verify that for each change to systems or networks: • A formal PCI DSS impact assessment was performed • PCI DSS requirements applicable to the system or network changes were identified • PCI DSS scope was updated as appropriate for the change • Sign-off by responsible personnel (as defined in A3.1.3) was obtained and documented	**Identify the change documentation examined** to verify that for each change to systems or networks: • A formal PCI DSS impact assessment was performed • PCI DSS requirements applicable to the system or network changes were identified • PCI DSS scope was updated as appropriate for the change • Sign-off by responsible personnel (as defined in A3.1.3) was obtained and documented	*<Report Findings Here>*				
	Identify the personnel interviewed who confirm that for each change to systems or networks: • A formal PCI DSS impact assessment was performed • PCI DSS requirements applicable to the system or network changes were identified • PCI DSS scope was updated as appropriate for the change • Sign-off by responsible personnel (as defined in A3.1.3) was obtained and documented	*<Report Findings Here>*				
A3.2.2.1 Upon completion of a change, all relevant PCI DSS requirements must be verified on all new or changed systems and networks, and documentation must be updated as applicable. Examples of PCI DSS requirements that should be verified include, but are not limited to: • Updated network diagram to reflect changes • Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled • Systems are protected with required controls, e.g. file integrity monitoring (FIM), anti-virus, patches, audit logging • Verification that sensitive authentication data (SAD) is not stored and that all cardholder data (CHD) storage is documented and incorporated into data retention policy and procedures • New systems are included in the quarterly vulnerability scanning process ***PCI DSS Reference:*** *Scope of PCI DSS Requirements; Requirement 1-12*			☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.2.2.1 For a sample of systems and network changes, examine change records, interview personnel and observe the affected systems/networks to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change.	**Identify the sample** of systems and network changes .	<*Report Findings Here*>				
	For the sample of systems and network changes:					
	Identify the change records examined to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change.	<*Report Findings Here*>				
	Identify the personnel interviewed who confirm that applicable PCI DSS requirements were implemented and documentation updated as part of the change.	<*Report Findings Here*>				
	Describe how the affected systems/networks were observed to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change.	<*Report Findings Here*>				
A3.2.3 Changes to organizational structure (for example, a company merger or acquisition, change or reassignment of personnel with responsibility for security controls) result in a formal (internal) review of the impact to PCI DSS scope and applicability of controls. ***PCI DSS Reference:*** *Requirement 12*			☐	☐	☐	☐
A3.2.3 Examine policies and procedures to verify that a change to organizational structure results in formal review of the impact to PCI DSS scope and applicability of controls.	**Identify the policies and procedures document(s) examined** to verify that a change to organizational structure results in formal review of the impact to PCI DSS scope and applicability of controls.	<*Report Findings Here*>				
A3.2.4 If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. ***PCI DSS Reference:*** *Requirement 11*			☐	☐	☐	☐
A3.2.4 Examine the results from the most recent penetration test to verify that: • Penetration testing to verify segmentation controls is	**Is segmentation in use? (yes/no)** *If no, mark the remainder of DE 2.4 as "not applicable."*	<*Report Findings Here*>				
	Identify the date of the most recent penetration test for which results are being examined.	<*Report Findings Here*>				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
performed at least 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 all out-of-scope systems from systems in the CDE.	*For the most recent penetration test,* **describe how examination of the results from the most recent penetration test** verify that:					
	• Penetration testing to verify segmentation controls is performed at least every six months and after any changes to segmentation controls/methods,	*<Report Findings Here>*				
	• The penetration testing covers all segmentation controls/methods in use	*<Report Findings Here>*				
	• The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.2.5 Implement a data discovery methodology to confirm PCI DSS scope and to locate all sources and locations of clear text PAN at least quarterly, and upon significant changes to the cardholder environment or processes. Data discovery methodology must take into consideration the potential for clear text PAN to reside on systems and networks outside of the currently defined CDE. ***PCI DSS Reference:*** *Scope of PCI DSS Requirements*			☐	☐	☐	☐
A3.2.5.a Examine documented data discovery methodology to verify the following: • Data discovery methodology includes processes for identifying all sources and locations of clear text PAN • Methodology takes into consideration the potential for clear text PAN to reside on systems and networks outside of the currently defined CDE.	**Identify the data discovery methodology document(s) examined** to verify that; • Data discovery methodology includes processes for identifying all sources and locations of clear text PAN • Methodology takes into consideration the potential for clear text PAN to reside on systems and networks outside of the currently defined CDE.	*<Report Findings Here>*				
A3.2.5.b Examine results from recent data discovery efforts, and interview responsible personnel to verify that data discovery is performed at least quarterly and upon significant changes to the cardholder environment or processes	**Describe the results from recent data discovery efforts examined** to verify that data discovery is performed at least quarterly and upon significant changes to the cardholder environment or processes.	*<Report Findings Here>*				
	Identify the personnel interviewed who confirm that data discovery is performed at least quarterly and upon significant changes to the cardholder environment or processes.	*<Report Findings Here>*				
A3.2.5.1 Ensure effectiveness of methods used for data discovery – e.g. methods must be able to discover clear text PAN on all types of system components (for example, on each operating system or platform) and file formats in use. The effectiveness of data discovery methods must be confirmed at least annually. ***PCI DSS Reference:*** *Scope of PCI DSS Requirements*			☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
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 clear text PAN on all types of system components and file formats in use	**Identify the personnel interviewed** who confirm that; • 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 clear text PAN on all types of system components and file formats in use	*<Report Findings Here>*				
	Identify the document(s) examined to verify that: • 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 clear text PAN on all types of system components and file formats in use	*<Report Findings Here>*				
A3.2.5.1.b Examine the results of recent effectiveness tests to verify the effectiveness of methods used for data discovery is confirmed at least annually.	**Identify the date(s) of the most recent effectiveness tests performed**, for which results were examined to verify that the effectiveness of methods used for data discovery is confirmed at least annually.	*<Report Findings Here>*				
A3.2.5.2 Implement response procedures to be initiated upon the detection of clear text PAN outside of the CDE to include: • Procedures for determining what to do if clear text PAN is discovered outside of the CDE, including its retrieval, secure deletion and/or migration into the currently defined CDE, as applicable • Procedures for determining how the data ended up outside of the CDE • Procedures for remediating data leaks or process gaps that resulted in the data being outside of the CDE • Procedures for identifying the source of the data • Procedures for identifying if any track data is stored with the PANs			☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.2.5.2.a Examine documented response procedures to verify that procedures for responding to the detection of clear text PAN outside of the CDE are defined and include: • Procedures for determining what to do if clear text PAN is discovered outside of the CDE, including its retrieval, secure deletion and/or migration into the currently defined CDE, as applicable • Procedures for determining how the data ended up outside the CDE • Procedures for remediating data leaks or process gaps that resulted in the data being outside of the CDE • Procedures for identifying the source of the data • Procedures for identifying any other track data stored with the PANs	**Identify the response procedures document(s) examined** to verify that procedures for responding to the detection of clear text PAN outside of the CDE are defined and include: • Procedures for determining what to do if clear text PAN is discovered outside of the CDE, including its retrieval, secure deletion and/or migration into the currently defined CDE, as applicable • Procedures for determining how the data ended up outside the CDE • Procedures for remediating data leaks or process gaps that resulted in the data being outside of the CDE • Procedures for identifying the source of the data • Procedures for identifying if any other track data is stored with the PANs	*<Report Findings Here>*				
A3.2.5.2.b Interview personnel and examine records of response actions to verify that remediation activities are performed when clear text PAN is detected outside of the CDE.	**Identify the personnel interviewed** who confirm that remediation activities are performed when clear text PAN is detected outside of the CDE.	*<Report Findings Here>*				
	Identify the records of response actions examined to verify that remediation activities are performed when clear text PAN is detected outside of the CDE.	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.2.6 Implement mechanisms for detecting and preventing clear text PAN from leaving the CDE via an unauthorized channel, method or process, including generation of audit logs and alerts. ***PCI DSS Reference:*** *Scope of PCI DSS Requirements*			☐	☐	☐	☐
A3.2.6.a Examine documentation and observe implemented mechanisms to verify that the mechanisms are: • Implemented and actively running • Configured to detect and prevent clear text PAN leaving the CDE via an unauthorized channel, method or process • Generating logs and alerts upon detection of clear text PAN leaving the CDE via an unauthorized channel, method or process	**Identify the document(s) examined** to verify that mechanisms are: • Implemented and actively running • Configured to detect and prevent clear text PAN leaving the CDE via an unauthorized channel, method *or process* • Generating logs and alerts upon detection of clear text PAN leaving the CDE via an unauthorized channel, method or process	*<Report Findings Here>*				
	Describe the implemented mechanisms observed to verify that mechanisms are: • Implemented and actively running • Configured to detect and prevent clear text PAN leaving the CDE via an unauthorized channel, method *or process* • Generating logs and alerts upon detection of clear text PAN leaving the CDE via an unauthorized channel, method or process	*<Report Findings Here>*				
A3.2.6.b Examine audit logs and alerts, and interview responsible personnel to verify that alerts are investigated.	**Identify the audit logs and alerts(s) examined** to verify that alerts are investigated.	*<Report Findings Here>*				
	Identify the responsible personnel interviewed who confirm that alerts are investigated.	*<Report Findings Here>*				
A3.2.6.1 Implement response procedures to be initiated upon the detection of attempts to remove clear text PAN from the CDE via an unauthorized channel, method or process. Response procedures must include: • Procedures for the timely investigation of alerts by responsible personnel • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss			☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.2.6.1.a Examine documented response procedures to verify that procedures for responding to the attempted removal of clear text PAN from the CDE via an unauthorized channel, method or process include: • Procedures for the timely investigation of alerts by responsible personnel • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss	**Identify the response procedures document(s) examined** to verify that procedures for responding to the attempted removal of clear text PAN from the CDE via an unauthorized channel, method or process include: • Procedures for the timely investigation of alerts by responsible personnel • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss	*<Report Findings Here>*				
A3.2.6.1.b Interview personnel and examine records of actions taken when clear text PAN is detected leaving the CDE via an unauthorized channel, method or process, and verify that remediation activities were performed	**Identify the personnel interviewed** who confirm that when clear text PAN is detected leaving the CDE via an unauthorized channel, method or process, remediation activities are performed	*<Report Findings Here>*				
	Identify the records of response actions examined to verify that when clear text PAN is detected leaving the CDE via an unauthorized channel, method or process, remediation activities were verified to have been performed	*<Report Findings Here>*				
A3.3 Validate PCI DSS is incorporated into business as usual (BAU) activities						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to: • firewalls • IDS/IPS • FIM • anti-virus • physical access controls • logical access controls • audit logging mechanisms • segmentation controls (if used) ***PCI DSS Reference:*** *Requirements 1-12*			☐	☐	☐	☐
A3.3.1.a Examine documented policies and procedures to verify that processes are defined to immediately detect and alert on critical security control failures.	**Identify the policies and procedures document(s) examined** to verify that processes are defined to immediately detect and alert on critical security control failures.	*<Report Findings Here>*				
A3.3.1.b Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	**Identify the detection and alerting process document(s) examined** to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	*<Report Findings Here>*				
	Identify the personnel interviewed who confirm that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.3.1.1 Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and document remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine if further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls ***PCI DSS Reference:*** *Requirements 1-12*			☐	☐	☐	☐
A3.3.1.1.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and document remediation required to address root cause • Identifying and addressing any security issues that arose during the failure	**Identify the policies and procedures document(s) examined** to verify that processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and document remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine if further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
• Performing a risk assessment to determine if further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	**Identify the personnel interviewed** who confirm that processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and document remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine if further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	*<Report Findings Here>*				
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 records of security control failures examined** 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	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.3.2 Review hardware and software technologies at least annually to confirm whether they continue to meet the organization's PCI DSS requirements. (For example, a review of technologies that are no longer supported by the vendor, and/or no longer meet the security needs of the organization.) The process includes a plan for remediating technologies that no longer meet the organization's PCI DSS requirements, up to and including replacement of the technology, as appropriate. ***PCI DSS Reference:*** *Requirement 2, 6*			☐	☐	☐	☐
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 policies and procedures document(s) examined** to verify that processes are defined and implemented to review hardware and software technologies to confirm whether they continue to meet the organization's PCI DSS requirements.	*<Report Findings Here>*				
	Identify the personnel interviewed who confirm that processes are defined and implemented to review hardware and software technologies to confirm whether they continue to meet the organization's PCI DSS requirements.	*<Report Findings Here>*				
A3.3.2.b Review the results of the recent reviews to verify reviews are performed at least annually.	**Identify the date(s) of the most recent reviews performed**, for which results were examined to verify that reviews are performed at least annually.	*<Report Findings Here>*				
A3.3.2.c For any technologies that have been determined to no longer meet the organization's PCI DSS requirements, verify a plan is in place to remediate the technology.	**Are there any technologies present that have been determined to no longer meet the organization's PCI DSS requirements? (yes/no)** *If no, mark the remainder of DE 3.2.c as "not applicable."*	*<Report Findings Here>*				
	If yes, **identify the technologies that have been determined to no longer meet the organization's PCI DSS requirements** and were verified to have a plan in place to remediate the technology.	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.3.3 Perform reviews at least quarterly to verify BAU activities are being followed. Reviews must be performed by personnel assigned to the PCI DSS compliance program (as identified in A3.1.3), and include the following: • Confirm that all BAU activities (e.g. A3.2.2, A3.2.6, and A3.3.1) are being performed • Confirm that personnel are following security policies and operational procedures (for example, daily log reviews, firewall rule-set reviews, configuration standards for new systems, etc.) • Document 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*			☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.3.3.a Examine policies and procedures to verify that processes are defined for reviewing and verifying BAU activities. Verify the procedures include: • Confirming that all BAU activities (e.g. A3.2.2, A3.2.6, and A3.3.1) are being performed • Confirming that personnel are following security policies and operational procedures (for example, daily log reviews, firewall rule-set reviews, configuration standards for new systems, etc.) • Documenting how the reviews were completed, including how all BAU activities were verified as being in place • Collecting documented evidence as required for the annual PCI DSS assessment • Reviewing and sign off of results by executive management assigned responsibility for PCI DSS governance • Retaining records and documentation, for at least 12 months, covering all BAU activities	**Identify the policies and procedures document(s) examined** to verify that processes are defined for reviewing and verifying BAU activities. Verify the procedures include: • Confirming that all BAU activities are being performed • Confirming that personnel are following security policies and operational procedures (for example, daily log reviews, firewall rule-set reviews, configuration standards for new systems, etc.) • Documenting how the reviews were completed, including how all BAU activities were verified as being in place • Collecting documented evidence as required for the annual PCI DSS assessment • Reviewing and sign off of results by executive management assigned responsibility for PCI DSS governance • Retaining records and documentation, for at least 12 months, covering all BAU activities	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.3.3.b Interview responsible personnel and examine records of reviews to verify that: • Reviews are performed by personnel assigned to the PCI DSS compliance program • Reviews are performed at least quarterly	**Identify the responsible personnel interviewed** who confirm that: • Reviews are performed by personnel assigned to the PCI DSS compliance program • Reviews are performed at least quarterly	*<Report Findings Here>*				
	Identify the records of reviews document(s) examined to verify that: • Reviews are performed by personnel assigned to the PCI DSS compliance program • Reviews are performed at least quarterly	*<Report Findings Here>*				
A3.4 Control and manage logical access to the cardholder data environment.						
A3.4.1 Review user accounts and access privileges to in-scope system components at least every six months to ensure user accounts and access remain appropriate, based on job function, and authorized. ***PCI DSS Reference:*** *Requirement 7*			☐	☐	☐	☐
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 personnel interviewed** who confirm 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	*<Report Findings Here>*				
	Identify the supporting document(s) examined 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	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.5 Identify and respond to suspicious events.						
A3.5.1 Implement a methodology for the timely identification of attack patterns and undesirable behavior across systems (for example, using coordinated manual reviews and/or using centrally-managed or automated log correlation tools) to include at least the following: • Identification of anomalies or suspicious activity as they occur • Issuance of timely 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*			☐	☐	☐	☐
A3.5.1.a Review documentation and interview personnel to verify a methodology is defined and implemented to identify attack patterns and undesirable behavior across systems in a timely manner, and includes the following: • Identification of anomalies or suspicious activity as they occur • Issuance of timely alerts to responsible personnel • Response to alerts in accordance with documented response procedures	**Identify the policies and procedures document(s) examined** to verify that a methodology is defined and implemented to identify attack patterns and undesirable behavior across systems in a timely manner, and includes the following: • Identification of anomalies or suspicious activity as they occur • Issuance of timely alerts to responsible personnel • Response to alerts in accordance with documented response procedures	*<Report Findings Here>*				
	Identify the personnel interviewed who confirm that a methodology is defined and implemented to identify attack patterns and undesirable behavior across systems in a timely manner, and includes the following: • Identification of anomalies or suspicious activity as they occur • Issuance of timely alerts to responsible personnel • Response to alerts in accordance with documented response procedures	*<Report Findings Here>*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
A3.5.1.b Examine incident response procedures and interview responsible personnel to verify that: • On-call personnel receive timely alerts • Alerts are responded to per documented response procedures	**Identify the incident response procedures document(s) examined** to verify that: • On-call personnel receive timely alerts • Alerts are responded to per documented response procedures	*<Report Findings Here>*				
	Identify the personnel interviewed who confirm that: • On-call personnel receive timely alerts • Alerts are responded to per documented response procedures	*<Report Findings Here>*				