Payment Card Industry (PCI)

Card Production and Provisioning Report on Compliance

Enter company name
Enter city name, Enter country name

Enter Assessor company name

For use with Physical Security Requirements – Appendix C: Security Operations Center v3.0.1

ROC Version 3.0.2

November 2023

Document Changes

Date	Version	Description
July 2015	1.0	Initial version
December 2015	1.0a	Minor errata
June 2016	1.0b	Expanded sections 2.2, 3.2 and 3.3
April 2017	2.0	Updated for changes incorporated into v2 of the Security Requirements, including Mobile Provisioning.
December 2017	2.1	Updated with addition of Test Procedures
June 2022	3.0	Updated for release of new Requirements
September 2022	3.0.1	Minor errata
November 2023	3.0.2	Minor errata

Contents

Introduction to the ROC Template

This document, the *PCI Card Production and Provisioning Report on Compliance for use with PCI Card Production and Provisioning Physical Security Requirements – Security Operations Center v3.0.1* ("ROC Reporting Template"), is the template for Payment Brand Assessors completing a Report on Compliance (ROC) for assessments against the *PCI Card Production and Provisioning Physical Security Requirements, Appendix C v3.0.1*

The ROC Reporting Template serves two purposes:

- It serves as a declaration of the results of the card vendor's assessment of compliance with the *PCI Card Production and Provisioning Physical Security Requirements – Security Operations Center v3.0.1*
- It provides reporting instructions and the template for assessors to use. This can help provide reasonable assurance that a consistent level of reporting is present among assessors.

Contact the requesting payment brand for reporting and submission procedures.

Use of this reporting template is subject to payment brand stipulations for all Card Production and Provisioning v3.0.1 submissions.

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. Additional appendices may be added if the assessor feels there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document.

Do not delete any content from any place in this document, including this section and the versioning above. These instructions are important for the assessor as the report is written and for the recipient in understanding the context from which the responses and conclusions are made. Addition of text or sections is applicable within reason, as noted above.

The Report on Compliance (ROC) is originated by the card vendor and further refined by the payment brand-designated assessor during the onsite card production and provisioning vendor assessment as part of the card vendor's validation process. The ROC provides details about the vendor's environment and assessment methodology, and documents the vendor's compliance status for each Card Production and Provisioning Security Requirement. A PCI Card Production and Provisioning Security compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment. The ROC is effectively a **summary of evidence** derived from the assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the ROC provides a comprehensive **summary of testing activities performed and information collected** during the assessment against the *PCI Card Production and Provisioning Physical Security Requirements v3.0*. The information contained in a ROC must provide enough detail and coverage to verify that the assessed entity is compliant with all PCI Card Production and Provisioning Security Requirements.

ROC Sections

The ROC includes the following sections and appendices:

1. Section 1: Contact Information and Report Date
2. Section 2: Summary of Non-Compliance Findings
3. Section 3: Inspection Overview
4. Section 4: Findings and Observations

Note: *Sections 1 through 4 must be thoroughly and accurately completed, in order for the assessment findings in Section 5 to have the proper context. The reporting template includes tables with reporting instructions built-in to help assessors provide all required information throughout the document. Responses should be specific but efficient. Information provided should focus on concise quality of detail, rather than lengthy, repeated verbiage. Parroting the testing procedure within a description is discouraged, as it does not add any level of assurance to the narrative. Use of template language for summaries and descriptions is discouraged and details should be specifically relevant to the assessed entity.*

ROC Vendor Self-Evaluation

The card vendor is asked to complete the card vendor self-evaluation in Section 5: Findings and Observations, for all requirements.

- Only one response should be selected at the sub-requirement level, and reporting of that should be consistent with other required documents.
- Select the appropriate response for “Compliant to PCI CP Requirement” for each requirement.
- In the “Comments/Remediation Date and Actions” section, the vendor may enter an explanation regarding its compliance that provides the payment brand assessor with additional information to be considered for the compliance assessment. In the event “No” is entered in the Compliance column, the vendor must state the planned remediation action and the date for the remediation. In the event "Not Applicable" is entered in the Compliance column, the vendor must explain why they believe the requirement does not apply for their situation.

ROC Summary of Assessor Findings

At each sub-requirement, under "Assessor Compliance Evaluation," there is a column in which to designate the result. There are five options to summarize the assessor's conclusion: Yes, New, Open, Closed, and Not Applicable.

The following table is a helpful representation when considering which selection to make and when to add comments. Remember, only one "Result" response may be selected at the sub-requirement level, and reporting of that should be consistent with other required documents.

Response	When to use this response:
Yes	Indicates the vendor is in compliance with this requirement
New	Indicates that this is a new non-compliance finding identified by the assessor for the first time.
Open	Indicates that this item was previously reported as a non-compliance finding and action (if any) taken by the vendor does not resolve the original condition. The "Non-Compliance Description" column must explicitly state when this finding was first reported, the non-compliance condition observed, and the action (or lack thereof) taken by the vendor to resolve the finding. Findings for which the vendor has taken corrective action that resolved the original finding but introduced new non-compliance condition are reported as new findings for the applicable requirement.
Closed	Indicates that this item was previously reported as a non-compliance finding and vendor corrective action has resolved the finding. The "Non-Compliance Description" column must describe the action the vendor has taken to resolve the finding.
Not Applicable	Indicates that the assessor's assessment confirms that the requirement does not apply to for the vendor. Not Applicable responses are only expected it the requirement applies to an activity that the vendor does not perform.
Comment/ Non-Compliance Assessment	Use this column to indicate: ▪ Clarification describing the conditions observed in support of the assessor's conclusion of compliance, or ▪ If non-compliance, a description of the reason for non-compliance. Note that specific payment brands may require additional supporting details where compliance is noted.

ROC Reporting Details

The reporting instructions in the Reporting Template explain the intent of the response required. There is no need to repeat the requirement or the reporting instruction within each assessor response. As noted earlier, responses should be specific and relevant to the assessed entity. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage and should avoid parroting of the requirement without additional detail or generic template language.

Do's and Don'ts: Reporting Expectations

DO:	*DON'T:*
▪ Use this Reporting Template when assessing against v3.0 of the Card Production and Provisioning Security Requirements. ▪ Complete all sections in the order specified. ▪ Read and understand the intent of each requirement and testing procedure. ▪ Provide a response for every security requirement. ▪ Provide sufficient detail and information to support the designated finding, but be concise. ▪ Describe *how* a Requirement was verified per the Reporting Instruction, not just that it *was* verified. ▪ Ensure all parts of the Reporting Instructions are addressed. ▪ Ensure the response covers all applicable system components. ▪ Perform an internal quality assurance review of the ROC for clarity, accuracy, and quality. ▪ Provide useful, meaningful diagrams, as directed.	▪ Don't simply repeat or echo the security requirement in the response. ▪ Don't copy responses from one requirement to another. ▪ Don't copy responses from previous assessments. ▪ Don't include information irrelevant to the assessment.

ROC Template for PCI Card Production and Provisioning Security Requirements v3.0

This template is to be used for creating a Report on Compliance. Content and format for a ROC is defined as follows:

1 Contact Information and Report Date

1.1 Contact Information

Client		
▪ Company name:		Payment Brand Identification Code:
▪ Company address:		
▪ Company URL:		
▪ Company contact:	Name:	
	Phone number:	E-mail address:
Assessor Company		
▪ Company name:		
▪ Company address:		
▪ Company URL:		
Assessor		
▪ Primary Assessor:	Name:	
	Phone number:	E-mail address:
▪ Secondary Assessor:	Name:	
	Phone number:	E-mail address:
▪ Secondary Assessor:	Name:	
	Phone number:	E-mail address:
Assessor Quality Assurance (QA) Primary Reviewer for this specific report *(not the QA Contact for the CPSA)*		
▪ QA Reviewer:	Name:	
	Phone number:	E-mail address:

1.2 Location, Date, and Timeframe of Assessment

▪ Address of facility where assessment was performed:		
▪ Date of Report (yyyy/mm/dd):		
▪ Timeframe of assessment (start date to completion date):	Start date (yyyy/mm/dd):	Completion date (yyyy/mm/dd):
▪ Was the review done onsite or remotely:	Select	
▪ If remotely, state the rationale:		
▪ If applicable, identify date(s) spent onsite at the entity:	Start date (yyyy/mm/dd):	Completion date (yyyy/mm/dd):

1.3 Monitored Facilities

Number of card production facilities monitored					
Location information of monitored card production facilities					
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	

Location information of monitored card production facilities *(continued)*					
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Business Address:			City:		
State/Province:		Country:		Postal Code:	

2. Summary of Non-Compliance Findings

Please use the table on the following page to report, covering all sections under each heading. Write up findings and list non-compliances—including the section reference number the non-compliance relates to—within the findings text as each non-compliance occurs. List all non-compliances in order, including the relevant section reference number the non-compliance—for example:

2.1 Non-Compliance Findings – Example

Requirement	New	Previous		Non-Compliance Findings Description
		Open	Closed	
C.2.1.a	☒	☐	☐	*The SOC is not located at a VPA-approved facility.*
C.5.2.1.b	☐	☒	☐	*The network topology diagram is not reviewed, updated, and verified at least once each year.*
C.5.15.g	☐	☐	☒	*Recovery procedures for an alternate SOC site do not require the site to be VPA approved prior to the initiation of SOC activities.*

Notes for Consideration

- *Please ensure non-compliances are written exactly as the examples above and be as specific as possible down to the exact bullet that covers the non-compliance.*
- *Also list items that are **not** non-compliances but are items that either the assessor is unsure of, or the vendor has discussed with the assessor and questions arising from this discussion can only be answered by the applicable payment brands(s). This section is optional, so if not required, please delete it from the report.*

2.2 Non-Compliance Findings – Detail

Requirement	New	Previous		Non-Compliance Findings Description
		Open	Closed	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	

Requirement	New	Previous		Non-Compliance Findings Description
		Open	Closed	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	

3. Inspection Overview

3.1 Facility Description

The auditor must provide a general description of the vendor facility and Card Production and Provisioning environment. For example, “The facility consists of multiple buildings, and card production activities are performed in one building consisting of a High Security Area for Card Production and Provisioning. Administration functions are performed external to the HSA. The vendor being audited is the only occupant of this building.”

The introduction must also include any unusual conditions that may impact the audit scope or compliance assessment process. For example, “First audit after relocation, significant expansion / reconfiguration of the HAS, significant changes to key personnel, introduction of new technologies,” and any other unusual conditions.

▪ Vendor Facility and Card Production and Provisioning Environment	
▪ Conditions that may Impact Audit Scope	

3.2 Documentation Reviewed

Identify and list all reviewed documents. Include the following:

Reference Number	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version)
Doc-1			
Doc-2			
Doc-3			
Doc-4			
Doc-5			
Doc-6			
Doc-7			
Doc-8			
Doc-9			
Doc-10			
Doc-11			
Doc-12			
Doc-13			
Doc-14			
Doc-15			
Doc-16			
Doc-17			
Doc-18			
Doc-19			
Doc-20			
Doc-21			
Doc-22			
Doc-23			
Doc-24			

Reference Number	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version)
Doc-25			
Doc-26			
Doc-27			
Doc-28			
Doc-29			
Doc-30			
Doc-31			
Doc-32			
Doc-33			
Doc-34			
Doc-35			
Doc-36			
Doc-37			
Doc-38			
Doc-39			
Doc-40			
Doc-41			
Doc-42			
Doc-43			
Doc-44			
Doc-45			
Doc-46			
Doc-47			
Doc-48			
Doc-49			
Doc-50			

3.3 Individuals Interviewed

Identify and list the individuals interviewed. Include the following:

Reference Number	Employee Name	Role/Job Title	Organization	Summary of Topics Covered / Areas or Systems of Expertise (high-level summary only)
Int-1				
Int-2				
Int-3				
Int-4				
Int-5				
Int-6				
Int-7				
Int-8				
Int-9				
Int-10				
Int-11				
Int-12				
Int-13				
Int-14				
Int-15				
Int-16				
Int-17				
Int-18				
Int-19				
Int-20				
Int-21				
Int-22				
Int-23				
Int-24				

Reference Number	Employee Name	Role/Job Title	Organization	Summary of Topics Covered / Areas or Systems of Expertise (high-level summary only)
Int-25				
Int-26				
Int-27				
Int-28				
Int-29				
Int-30				
Int-31				
Int-32				
Int-33				
Int-34				
Int-35				
Int-36				
Int-37				
Int-38				
Int-39				
Int-40				
Int-41				
Int-42				
Int-43				
Int-44				
Int-45				
Int-46				
Int-47				
Int-48				
Int-49				
Int-50				

4. Validating the Requirements

The validation methods identified for each requirement describe the expected activities to be performed by the assessor to validate whether the entity has met the requirement. The intent behind each validation method is described as follows:

- **Examine:** The assessor critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.
- **Observe:** The assessor watches an action or views something in the environment. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, system configurations/settings, environmental conditions, and physical controls.
- **Interview:** The assessor converses with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.

The validation methods are intended to allow the assessed entity to demonstrate how it has met a requirement. They also provide the assessed entity and the assessor with a common understanding of the assessment activities to be performed. The specific items to be examined or observed and personnel to be interviewed should be appropriate for the requirement being assessed, and for each entity's particular implementation.

When documenting the assessment results, the assessor identifies the validation activities performed and the result of each activity. While it is expected that an assessor will perform all the validation methods identified for each requirement, it is also possible for an implementation to be validated using different or additional methods. In such cases, the assessor should document why they used validation methods that differed from those identified in this document.

5. Findings and Observations

Section C.1: General Requirements

Section C.1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
a) Only activities related to SOC and SCR operations shall occur within the SOC perimeter. ***Note:*** *SCR activities are not required to occur within the SOC environment.*	Select		Observe to verify that only activities related to SOC and SCR operations occur within the SOC perimeter. Interview personnel to verify that only activities related to SOC and SCR operations occur within the SOC perimeter.	Select	
b) SOCs must only monitor facilities that are owned and operated by the card vendor who operates the SOC.	Select		Examine documentation to verify that facilities monitored are owned and operated by the card vendor who operates the SOC. Interview personnel to verify that the SOC only monitors facilities that are owned and operated by the card vendor who operates the SOC.	Select	
c) SOCs must only monitor card production facilities that are either VPA-approved or are seeking VPA approval.	Select		Examine documentation to identify which vendor facilities are VPA-approved and list them for VPA review.	Select	
d) There must be a shared, common spoken language between all SOCs and managed vendor facilities that all SOC personnel and security responders—i.e., local onsite staff—can use to communicate.	Select		Examine applicable policies and procedures to verify that a shared common spoken language exists between all SOCs and managed vendor facilities. Interview a sample of personnel to verify they can speak the language.	Select	
e) Upon initiation of communication from a SOC, a trained member of the security organization—e.g., security manager, CISO, security responder—must respond within two minutes when required to intervene in an active event.	Select		Examine policies and procedures to verify that a trained member of the security organization must respond within two minutes when required to intervene in an active event.	Select	

Section C.1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) Security responders must be onsite whenever a managed vendor facility is operational. These personnel must be trained to the same level as security guards, as defined in this document.	Select		Examine applicable policies and procedures to verify that security responders must be onsite whenever a managed vendor facility is operational and that they must be trained to the same level as security guards as defined in this document. Interview a sample of security responders to verify that they must be onsite whenever a managed vendor facility is operational and that they are trained to the same level as security guards.	Select	
g) The SOC personnel must be aware of who to contact whenever a facility is operational. This information must be readily available at all times for the SOC personnel. This includes but not limited to: • Production manager • Local security manager • CISO • Security Responder(s) This must be reviewed on a monthly basis by the Local Security Manager and provided to the SOC. The SMS must be updated with this information within 48 hours of receipt.	Select		Examine policies and procedures to verify information is provided to SOC personnel of who contact whenever a facility is operational and that this includes: • Production manager • Local security manager • CISO • Security Responder(s) Interview a sample of SOC personnel to verify their awareness of the aforementioned. Examine policies and procedures to verify that the contact information is reviewed on a monthly basis by the Local Security Manager and provided to the SOC. Examine policies and procedures to verify the security management system is updated within 48 hours of receipt of this information.	Select	
h) All staff that have access to a managed vendor facility must be able to contact the SOC.	Select		Interview a sample of staff with access to a managed vendor facility to verify they have the ability to contact the SOC	Select	

Section C.1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
The vendor must:					
i) Document security controls that protect security system data and the SOC network.	Select		Examine policies and procedures to verify that security controls for protecting security system data and the SOC network exists.	Select	
j) Ensure that any system used in the SOC process is only used to perform its intended function—i.e., monitor and control SOC process activities and/or provide administration activities.	Select		Interview SOC personnel to verify that systems used in the SOC process are only used to perform intended functions.	Select	
k) Change supplier provided default parameters prior to or during installation in the SOC environment.	Select		Examine documentation to verify that supplier provided default parameters are changed prior to or during installation into the SOC environment.	Select	
l) Synchronize clocks on all systems-associated SOC networks with an external time source based on International Atomic Time or Universal Time Coordinated (UTC).	Select		Examine documentation to verify that all systems-associated SOC network clocks are synchronized with an external time source based on International Atomic Time or Universal Time Coordinated (UTC).	Select	
m) Restrict and secure access to security system files at all times.	Select		Examine access controls to security system files to verify access is restricted to only authorized personnel.	Select	

Section C.2: Physical Construction

Section C.2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
To ensure that the SOC can provide effective management of a managed vendor facility, the SOC has a resilient infrastructure—i.e., its physical location, structural requirements, equipment within the SOC, and layout.					
C.2.1 SOC location					
The vendor must ensure the SOC:					
a) Is located at a VPA-approved facility.	Select		Observe that the SOC is located in a VPA-approved facility	Select	
b) Is outside of the high security area (HSA) of the facility and the cloud-based provisioning environment and is segregated from the Security Control Room (SCR), either in a separate room, or a fully segregated room within the SCR, or a stand-alone building.	Select		Observe the location of the SOC to verify that it is located outside of the HSA and cloud-based provisioning environment and is segregated from the SCR either in a separate room or a fully segregated room within the SCR, or a stand-alone building.	Select	
c) Is in a building with low risk of fire, explosion, flooding, vandalism, and exposure hazards from other buildings, and the vendor has performed an analysis to demonstrate that mitigation. The building must be protected against the effects of lightning strikes.	Select		Examine the vendor's analysis to verify the mitigations have been identified. Observe the building housing the SOC to verify it is located in a building that has a low risk of fire, explosion, flooding, vandalism, and exposure hazards from other buildings and the mitigations identified have been implemented. Observe that the building has protections against the effects of lightning strikes.	Select	

Section C.2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.2.2 Structural requirements					
The vendor must ensure that:					
a) The perimeter walls of the SOC must be concrete or of a similar construction of equivalent resistance.	Select		Examine documentation for the design of the SOC perimeter walls to verify they are constructed of concrete or a similar construction of equivalent resistance. Observe the perimeter walls to verify the design is constructed as stated above.	Select	
b) Doors, frames, locks, and door closers fitted with ACS must all be of reasonable quality and strength to be effective.	Select		Observe the doors, frames, locks, and door closers fitted with ACS to verify the construction are of reasonable quality and strength to be effective	Select	
c) Fail-secure doors must be used that will not release in the event of emergency egress or power failure—i.e., the default state is the door stays locked.	Select		Observe that fail-secure doors are used for the SOC that do not release in the event of emergency egress or power failure.	Select	

Section C.2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) A Hostile Vehicle Mitigation (HVM) risk assessment must be performed to ensure the risk of a vehicle penetrating the SOC is mitigated. Controls to be considered in the risk assessment are: • Location of the SOC in relation to distance from vehicular access points. • Walls existing between the SOC and the road. • Installation of HVM Barriers. The vendor must ensure the following: • All risks identified that could result in a breach of the SOC are remediated. • Assessment is reviewed on an annual basis.	Select		Examine documentation of the HVM risk assessment to verify controls mitigating the risk of a vehicle penetrating the SOC have been considered. Examine evidence that the assessment is reviewed on an annual basis. Interview a local security manager to verify that all risks identified that could result in a breach of the SOC are remediated and that the assessment is reviewed on an annual basis.	Select	
e) All external windows are to be physically secure from external attack—e.g., non-opening, bullet-resistant, or equipped with metal bars. Windows will be mirrored or use material such as opaque film to prevent sight into buildings.	Select		Observe to determine external windows, doors, and other openings are protected against intrusion by mechanisms such as intruder-resistant (e.g., "burglar-resistant") glass, bars, glass-break detectors, or motion or magnetic contact detectors and are mirrored or use material such as opaque film to prevent sight into buildings.	Select	
f) External lighting is used to assist in protecting the SOC in conjunction with the CCTV to protect the perimeter.	Select		Observe CCTV footage to verify that external lighting assists in protecting the SOC perimeter in conjunction with CCTV.	Select	
g) Entrance to the SOC must be via an access-controlled mantrap.	Select		Observe that the entrance to the SOC is controlled via an access-controlled mantrap.	Select	
h) Entrance to the SOC must be fitted with an intercom.	Select		Observe that the entrance to the SOC is fitted with an intercom.	Select	

Section C.2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) CCTV must cover all areas of the SOC, as well as its entrances and exits, as defined in Section 2.4.5, "Closed Circuit Television (CCTV)."	Select		Examine security-control documentation to verify the SOC has CCTV coverage as defined in Section 2.4.5, "Closed Circuit Television (CCTV)." Observe to verify the SOC is covered by CCTV as defined in Section 2.4.5, "Closed Circuit Television (CCTV)."	Select	
j) The SOC must be protected with a sufficient number of intruder-detection devices that provide an early attack indication—e.g., seismic, vibration/shock, microphonic wire, microphone, etc.—on attempts to enter, as well as full coverage of the walls, ceiling, and floor.	Select		Examine documentation to verify the SOC has a sufficient number of intruder-detection devices that provide early attack indication—e.g., seismic, vibration/shock, microphonic wire, microphone, etc.—for any attempts to enter as well as full coverage of the walls, ceiling, and floor. Observe access to the SOC to verify the intruder-detection devices are installed as documented.	Select	
k) The SOC is protected by internal motion detectors that must be activated in zones whenever no authorized staff are known to be present.	Select		Observe the SOC and all separate rooms within the SOC to verify they are protected by internal motion detectors that must be activated in zones when no staff are present. Observe via inspection that every zone has motion detectors installed, and open-plan areas have sufficient devices installed to ensure motion will be detected by someone walking through the area (100% coverage is not required).	Select	

Section C.2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.2.3 Equipment within the SOC *The SOC has the equipment that is sufficient to adequately monitor the sites that that are under SOC control, with the capability to expand if and when required. The number of operators and workstations needed will be determined by the time required to manage all events from the sights monitored by the SOC.*					
At a minimum, each SOC must have:					
a) Sufficient operator workstations and monitors to address the following: • Displaying at a minimum: – Event management – Standard operating procedures – CCTV • Ability from a single console to achieve single-point control of systems	Select		Observe to verify that the SOC has sufficient operator workstations, to address the following: • Displaying at a minimum: – Event management – Standard operating procedures – CCTV • Ability from a single console to achieve single-point control of systems	Select	
b) Two independent forms of communication	Select		Observe to verify that the SOC has sufficient operator workstations to address two independent forms of communication.	Select	
c) Duress alarm buttons	Select		Observe to verify that the SOC has sufficient operator workstations to address duress alarm buttons.	Select	
d) An intrusion alarm panel for management of the SOC alarm system, and investigation of events. The alarm system must automatically arm and disarm based on the authorized occupancy of the room. For example, zero occupancy auto-arms the system and occupancy of one or greater auto-disarms the system.	Select		Observe to verify that the SOC has an intruder alarm panel for management of the SOC alarm system, and investigation of events. Examine documentation to verify that the alarm system automatically arms and disarms based on the authorized occupancy of the room.	Select	

Section C.2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) A security video wall to allow a collaborative environment and for background topics to view international news channels, incidents, events. The monitor wall must be sufficient for any SOC operator to observe.	Select		Observe to verify that the SOC has a security video wall with sufficient monitors to allow a collaborative environment and for background topics.	Select	

Section C.2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.2.4 Layout of the SOC *The SOC is configured with the equipment and personnel necessary to effectively monitor the activities and control access at remote facilities.* *There are at a minimum three main areas as described below.* **Mantrap Entrance** *The mantrap controls access to the SOC and minimizes disruption to critical business activities.* **Monitoring room** *The main purpose of the monitoring room is to provide a well-managed, ergonomic area for SOC operators to effectively manage all security system events across the managed vendor facilities. The monitoring room will:* • *Provide effective access control and monitoring of PCI CPP regulated areas.* • *Provide resilience and redundancy of critical SMS.* • *Initiate appropriate and timely security response to incidents.* • *Oversee security responses until resolved and provide post-incident reporting.* **Investigation room** *There is dedicated investigations room, separate from the SOC monitoring room.* *Without disturbing the day-to-day operations, the purpose of this area is to:* • *Provide a quiet area to concentrate on high-level event management.* • *Host third parties as part of an investigation.* • *Host third parties for the purpose of auditing.*					
The SOC must have:					
a) A mantrap entrance to prevent staff “piggybacking” or tailgating (excluding emergency exits).	Select		Observe entrances and exits to determine whether they are fitted with a mantrap to prevent staff “piggybacking” or tailgating (excluding emergency exits).	Select	

Section C.2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) A monitoring room, where event monitoring is conducted.	Select		Observe that the SOC has an event monitoring room.	Select	
c) An investigation room for more in-depth reviews, demonstrations, or audits of the system, without disturbing the monitoring room.	Select		Observe that the SOC has an investigation room that can be used without disturbing the monitoring room.	Select	

Section C.3: Security Management System

Section C.3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
A Security Management System (SMS) needs to be created by integrating all the managed vendor facility security systems together to form a centralized operational and management system. The SMS is to be designed to provide real-time information and events to the SOC. For example, an active event, such as a perimeter alarm, will generate an alarm in the SOC. A graphical map will then display the location of the alarm, and the most relevant camera images will appear on the workstation monitors. This will quickly provide the SOC operator with all the information required to investigate potential incidents and initiate appropriate responses.					
C.3.1 SMS Provisions					
The SMS must provide:			Observe to verify that the SMS provides for:		
a) Visual verification of alarms when possible, to identify nuisance alarms or to initiate an appropriate and balanced response to an actual incident.	Select		• Visual verification of alarms to identify nuisance alarms or to initiate a response to an actual incident.	Select	
b) Events must be monitored using a video wall in combination with SOC operator workstations.	Select		• Events are monitored using a video wall in combination with SOC operator workstations.	Select	
c) Single graphical user interface (GUI) to allow the global estate, sites and buildings to be fully monitored.	Select		• Single graphical user interface (GUI) to allow the global estate, sites and buildings to be fully monitored.	Select	
d) Display pertinent information displayed to aid SOC monitoring and allow a quicker response to incidents.	Select		• Pertinent information displayed to aid SOC monitoring and allow a quicker response to incidents.	Select	

Section C.3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Collection of system data for reports and to provide intelligence to the security management.	Select		• Collection of system data for reports and to provide intelligence to the security management.	Select	
f) Secure connection to third-party databases to allow for single sourcing of data to reduce errors.	Select		• Secure connection to third-party databases to allow for single sourcing of data to reduce errors.	Select	
C.3.2 System Baseline Requirements					
a) The SMS must:			Examine documentation to verify the SMS:		
i. Allow for real-time event monitoring.	Select		Allows for real-time event monitoring	Select	
ii. Integrate with security systems to provide pop-ups for event management.	Select		Integrates with security systems to provide pop-ups for event management	Select	
iii. Support secure individual log-on with configurable user privileges, including user, operator, supervisor, and administrator.	Select		Supports secure individual log-on with configurable user privileges	Select	
iv. Provide search functions for reporting and audit purposes to include, but not limited to event logs, user transactions and alarms.	Select		Provides search functions for reporting and auditing, including event logs, user transactions and alarms	Select	
v. Allow viewing of system events when required.	Select		Allows viewing of system events when required.	Select	

Section C.3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) The CCTV system must be able to: • View both live and recorded CCTV footage. • Automatically display live CCTV footage associated to an event. • Display recorded CCTV footage that is marked at the event ready for playback.	Select		Examine documentation to verify the CCTV system can • View both live and recorded CCTV footage. • Automatically display live CCTV footage associated to an event. • Display recorded CCTV footage that is marked at the event ready for playback Observe to verify that the aforementioned CCTV system characteristics exist.	Select	
c) Each SOC must have sufficient bandwidth to manage the security systems. • Minimum requirements include the capability to simultaneously stream the following: – Multiple CCTV feeds per SOC operator workstation. – Multiple CCTV feeds per supervisor workstation. – Multiple CCTV feeds per manager workstation. • This must be tested on a monthly basis.	Select		Examine documentation to verify the SOC has sufficient bandwidth to manage security systems including providing for the following minimums: • Multiple CCTV feeds per SOC operator workstation. • Multiple CCTV feeds per supervisor workstation. • Multiple CCTV feeds per manager workstation. Observe to verify that the aforementioned minimum feeds exist at each applicable workstation	Select	

Section C.3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Standard operating procedures must be creating for the management of all security systems events. The event log must include: • Definition of action required. • Person completing the action. • Time and date action was completed.	Select		Examine documentation of standard operating procedures for management of all security system events to verify their existence. Examine a sample of the event log to verify that it contains the following: • Definition of action required. • Person completing the action. Time and date action was completed.	Select	
C.3.3 Functionality *From the SOC Monitoring room, the SOC operators are able to manage all security system events from any site being monitored.*					
C.3.3.1 Security System Events					
The following events must be logged:			Examine a sample of security system event logs to verify they contain the following information at a minimum:		
a) Unauthorized access attempts	Select		Unauthorized access attempts	Select	
b) Access (successful or failed) attempts results	Select		Access attempts results	Select	
c) Anti-pass-back violations	Select		Anti-pass-back violations	Select	
d) Door-open-too-long alarm	Select		Door-open-too-long alarm	Select	
e) Forced door	Select		Forced door	Select	

Section C.3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) Occupancy violations such as: • Dual occupancy • Occupancy greater or equal to one, with no motion detected within 15 or fewer minutes • Motion detected when occupancy equals zero • Motion detected inside the inner room of the loading bay when both intermediate and inner doors are closed	Select		Occupancy violations such as: • Dual occupancy • Occupancy greater or equal to one, with no motion detected within 15 or fewer minutes • Motion detected when occupancy equals zero Motion detected inside the inner room of the loading bay when both intermediate and inner doors are closed	Select	
g) Duress Alarm activation	Select		Duress Alarm activation	Select	
h) 24/7 monitored intruder alarm device activation	Select		24/7 monitored intruder alarm device activation	Select	
i) Activations from managed vendor facilities where intruder alarm systems are set	Select		Activations from managed vendor facilities where intruder alarm systems are set	Select	
j) Intruder alarm system not set or unset within a scheduled time	Select		Intruder alarm system not set or unset within a scheduled time	Select	
k) Fire alarm activation	Select		Fire alarm activation	Select	
l) Auxiliary power or battery backup system is invoked	Select		Auxiliary power or battery backup system is invoked	Select	
m) CCTV involuntary or voluntary disconnection	Select		CCTV involuntary or voluntary disconnection	Select	

Section C.3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.3.3.2 Access Credential Management					
SOC personnel can be authorized to create or update access credentials for the managed vendor facilities. The vendor must first ensure that:					
a) The Access Credential Management Process must include: • A request for updating access credentials is made. • The local security manager or other authorized personnel within each managed vendor facility approves the change. • The request is sent to the SOC, and SOC personnel modify the access credential assignment under dual control. • All changes to the system must be logged.	Select		Examine policies and procedures to verify the following processes exist • A request for updating access credentials is made. • The local security manager or other authorized personnel within each managed vendor facility approves the change. • The request is sent to the SOC, and SOC personnel modify the access credential assignment under dual control. • All changes to the system are logged. Examine a sample of creation and updating of access credentials to verify the aforementioned process is followed.	Select	
C.3.3.3 Event Management Steps					
a) An "Event matrix" must be created. The matrix must: • List all possible events for each system type. • For each event type, an SLA must be established.	Select		Examine documentation to verify that an event matrix has been created that includes: • Listing all possible events for each system type • For each event type an SLA is established	Select	

Section C.3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) For each identified event: • The event must be registered in the security system and actioned by the SOC operator. • The system must automatically bring all relevant information—e.g., event information (alarm location depicted on map), CCTV live and recorded footage, and standard operating procedures—to a selection of screens in front of the SOC operator. • Documented procedures must require the SOC operator to investigate the event.	Select		Examine security system documentation to verify: • Events are registered in the security system and actioned by the SOC operator • That the system automatically brings all relevant information (e.g., event information, CCTV live and recorded footage, and standard operating procedures) to a selection of screens in front of a SOC operator. Examine policies and procedures to verify that SOC operators are required to investigate events. Interview a SOC operator to verify the event investigation process defined above.	Select	
c) Documented procedures must provide guidance to facilitate operator taking action to: • Contain the event. • Escalate as necessary. • Take necessary corrective actions within prescribed time frames.	Select		Examine documentation of standard operating procedures to verify they contain guidance for SOC operator actions required to contain events and prevent their escalation. Observe that SOC operators have systems available in front of them to contain an event, including blocking access rights or alerting the local security manager. Examine documentation of standard operating procedures to verify they contain guidance for SOC operators on necessary corrective actions.	Select	
d) The system must help generate a report by automatically pulling the relevant data into one template.	Select		Examine a sample of medium- and high-security events to verify that the security system automatically generates a report pulling the relevant data into one template.	Select	

Section C.3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Documented procedures must require that all actions taken for medium- and high-security events are reviewed to ensure that the preventative actions are sufficient to prevent reoccurrence.	Select		Examine policies and procedures of to verify that medium- and high-security events are reviewed to ensure that the preventative actions taken are sufficient to prevent reoccurrence.	Select	
C.3.4 Priorities *The system processes the events on a priority basis to allow efficient and effective management. The guideline timing below provides the first steps to contain the event and prevent it from escalating. Subsequent steps can take longer, based on other events.*					
a) All security system events must be addressed within the following timeframes: • N/A events are simply registered without action. • Low priority events must be addressed within 30 minutes. • Medium priority events must be addressed within 10 minutes. • High priority events must be addressed within 6 minutes.	Select		Examine policies and procedures to verify they require that security system events are contained according to the following timeframes: • N/A events are simply registered without action. • Low priority events are addressed within 30 minutes. • Medium priority events are addressed within 10 minutes. • High priority events are addressed within 6 minutes. Examine a sample of low, medium, and high priority events to verify they are addressed within the prescribed timeframes.	Select	

Section C.3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.3.4.1 Performance Management					
a) Ongoing performance must be monitored and reported, ensuring: • The event matrix is accurate and kept up to date. • Events are managed correctly within the SLA's defined in the event matrix. • The Corporate Security Director reports the results of SLA performance on a monthly basis to senior management. • The full assessment is reviewed annually.	Select		Examine policies and procedures to verify a process exists and is followed to ensure the event matrix is kept accurate and up to date. Examine a sample of events to verify they are managed within the specifications of the SLA as defined in the event matrix. Interview the Corporate Security Director to verify the CSD reports the results of SLA performance on a monthly basis to senior management. Examine policies and procedures to verify the full assessment is reviewed annually.	Select	

Section C.4: SOC Personnel

Section C.4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
a) A corporate security director must be designated to ensure oversight and continuity between all SOCs of the vendor. • This position is responsible for ensuring that: • The SOCs are appropriately resourced. • The SOCs fulfil their responsibility for the remote monitoring and administration of all managed vendor facilities. • The corporate security director must report to senior management the status and performance of the SOCs on a quarterly basis.	Select		Examine applicable policies and procedures to verify that a senior manager has been designated as corporate security director to ensure oversight and continuity between all SOCs of the vendor. Interview the corporate security director to determine their understanding of their roles and responsibilities, which include: • The SOCs are appropriately resourced. • The SOCs fulfil their responsibility for the remote monitoring and administration of all managed vendor facilities. • Reporting to senior management the status and performance of the SOCs on a quarterly basis.	Select	
b) The corporate security director must be an employee of the vendor.	Select		Examine employment documentation to verify employment and position.	Select	
c) A CISO must be designated to be responsible for all security matters related to the SOC.	Select		Examine applicable policies and procedures to verify that a senior manager has been designated as CISO responsible for all security matters related to the SOC. Interview the CISO to determine their understanding of their roles and responsibilities.	Select	
d) The CISO must be an employee of the vendor.	Select		Examine employment documentation to verify employment and position.	Select	

Section C.4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) A dedicated supervisor must be working in a SOC whenever the SOCs are operational. The supervisor's role is: • Coordinating incident management responses. • Functioning as the initial point of escalation of security events for the SOCs.	Select		Examine applicable policies and procedures to verify that individuals have been designated as dedicated supervisors to work in the SOC whenever the SOCs are operational. Interview at least one dedicated supervisor to determine his or her understanding of roles and responsibilities which include: • Coordinating incident management responses. • Functioning as the Initial point of escalation of security events for the SOCs.	Select	
f) The dedicated supervisors must be employees of the vendor.	Select		Examine employment documentation to verify employment and position.	Select	
g) Each SOC must be manned by the appropriate number of SOC operators according to Section C.2.3.3, "Event Management Steps." At a minimum, there must always be one SOC operator per operational SOC location.	Select		Examine applicable policies and procedures to verify that each SOC must be manned by the appropriate number of SOC operators according to Section C.2.3.3, "Event Management Steps." At a minimum, there must always be one SOC operator per operational SOC location. Observe the SOC at the facility under review to verify that the number of SOC operators is in accordance with Section C.2.3.3, "Event Management Steps".	Select	

Section C.4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) Supervisors and SOC operators are not permitted to perform any functions normally associated with the production of card products or card components. They must not have access to: • HSAs • Physical Master Keys that provide access to card production or provision environments • Any restricted areas where the vendor processes, stores, or ships or receives card products and card components	Select		Examine applicable policies and procedures to verify that supervisors and SOC operators are not permitted to perform any functions normally associated with the production of card products or card components including access to: • HSAs • Physical Master Keys that provide access to card production or provision environments • Any restricted areas where the vendor processes, stores, or ships or receives card products and card components Interview a sample of supervisors and SOC operators to determine their understanding of their roles and responsibilities which DO NOT include access to: • HSAs • Physical Master Keys that provide access to card production or provision environments Any restricted areas where the vendor processes, stores, or ships or receives card products and card components.	Select	

Section C.5: Data Security

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.5.1 Communication between SOC and Managed Vendor Facilities					
Communication between SOC and managed vendor facilities must use HTTPS connections (to ensure security of communication is maintained while firewalls ensure specific flows for inbound/outbound traffic. These connections must:					
a) Use authorized locations and equipment to be defined and managed accordingly.	Select		Examine policies and procedures to verify that only authorized locations and equipment are used.	Select	
b) Use strong cryptography and security protocols to safeguard security system data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	Select		Examine documentation and system settings to verify that only strong cryptography and security protocols as defined in PCI DSS are used for transmission of security system data over open, public networks. This includes: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.5.2 Network Security *Access-control information, CCTV images, and any other data used in connection with remote administration of a card facility are encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit.* *Secure transmission of security system data requires using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt security system data. Connection requests from systems that do not support the required encryption strength and would result in an insecure connection should not be accepted.* *Note that some protocol implementations (such as SSL, SSH v1.0, and TLS 1.0 or 1.1) have known vulnerabilities that an attacker can use to gain control of the affected system. Whichever security protocol is used, ensure it is configured to use only secure versions and configurations to prevent use of an insecure connection—e.g., using only trusted certificates and supporting strong encryption, not weaker, insecure protocols or methods.* *Verifying that certificates are trusted—e.g., have not expired and are issued from a trusted source—helps ensure the integrity of the secure connection.* *Generally, the web page URL should begin with "HTTPS" and/or the web browser with a padlock icon displayed somewhere in the window. Many TLS certificate vendors also provide a highly visible verification seal—sometimes referred to as a "security seal," "secure site seal," or "secure trust seal"—which may provide the ability to click on the seal to reveal information about the website.* *Refer to industry standards and best practices for information on strong cryptography and secure protocols—e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.* **Note:** SSL/early TLS is not considered strong cryptography and may not be used as a security control.					
C.5.2.1 General Requirements					
The vendor must:					
a) Maintain a current network topology diagram that includes all system components on the network. The diagram must clearly define the boundaries of all networks.	Select		Examine network topology diagram to verify it exists, clearly defines the boundaries for all networks, and includes all system components related to the SOC.	Select	
b) Ensure the network topology diagram is reviewed, updated as appropriate, and verified at least once each year and whenever the network configuration is changed.	Select		Interview network administration personnel to verify the policy and procedures require topology review and update upon making changes to the network and at least annually. Examine evidence that the network topology diagram was reviewed and updated when the network configuration was changed and at least within the last 12 months if there were no changes.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Ensure that the CISO accepts, by formal signature, the security implications of the current network topology.	Select		Examine evidence that the CISO has accepted the security implications of the current network topology and that the document includes his or her formal signature.	Select	
d) Document the flow of security system data within the environment from the receipt/generation to end of its lifecycle.	Select		Examine the data-flow diagram of security system data within the environment from the receipt/generation to end of its lifecycle. Interview the IT manager to verify the diagram(s) are kept current and updated as needed.	Select	
e) Ensure that the SMS is on dedicated network(s) independent of the back office—e.g., accounting, human resources, etc.—and Internet-connected networks.	Select		Examine documentation to verify that the SMS is on dedicated network(s) independent of the back office.	Select	
f) Put controls in place to restrict, prevent, and detect unauthorized access to the security system networks.	Select		Examine policies and procedures to verify that access to the security system networks is restricted, and unauthorized access is prevented and detected. Examine a sample of access rules to verify that access to the security system networks is restricted, and unauthorized access is prevented and detected.	Select	
g) Be able to immediately assess the impact if any of its critical connecting points are compromised.	Select		Examine documented incident response procedures to verify processes are in place that allow for immediate assessment of the impact of any compromise of critical connecting points	Select	
h) Control at all times the physical connection points leading into the security system network.	Select		Observe physical connection points leading into the security system network to verify they are controlled at all times.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) Prevent data from being tampered with or monitored by protecting the network cabling associated with security system data movement.	Select		Observe a sample of security system network cabling to verify that access is restricted, the cabling is protected, and safeguards are in place to avoid tampering.	Select	
j) Ensure a process is in place for updates and patches and identification of their criticality, as detailed in Section C.6.14, "Configuration and Patch Management."	Select		Examine documented procedures to verify they include a process for updates and patches that includes identification of their criticality as delineated in the Section C.6.14, "Configuration and Patch Management."	Select	
k) Have the capability to detect, isolate, and correct abnormal operations within the SMS network endpoints on a real-time basis, 24/7.	Select		Interview personnel to verify that system-monitoring assets are functional and utilized. Examine evidence to verify that abnormal operations on SMS network endpoints can be: • Detected, • Isolated, and • Corrected on a real-time and 24/7 basis.	Select	
C.5.3 Network Devices *The requirements in this section apply to all hardware—e.g., routers, controllers, firewalls, storage devices—that comprises the security system networks.*					
The vendor must:					
a) Document the process to authorize all changes to network devices and protocols.	Select		Examine policies and procedures to verify a process is in place to authorize all changes to network devices and protocols prior to implementation. Examine a sample of change-management logs for network devices and protocols to verify the changes are authorized.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Document the current network device configuration settings, rules set and justification for each device.	Select		Examine a sample of network device documentation to verify configuration settings, rulesets, and their justifications are documented. Interview personnel to verify they are familiar with the documentation and process by which the documentation is updated.	Select	
c) Ensure all available services are approved by an authorized security manager.	Select		Interview personnel to identify available services. Examine evidence that available services were approved by an authorized security manager.	Select	
d) Implement logical and physical security controls that protect the integrity of network devices used.	Select		Examine documentation of logical and physical security controls that protect the integrity of network devices used to verify existence. Observe a sample of the controls to verify effective implementation.	Select	
e) Implement mechanisms to effectively monitor activity on network devices.	Select		Interview personnel to verify mechanisms are defined and implemented to effectively monitor the activity on network devices. Examine policies and procedures to verify mechanisms are defined to effectively monitor the activity on network devices.	Select	
f) Implement patches in compliance with Section C.6.14, “Configuration and Patch Management.”	Select		Examine a sample of device configurations and verify that patches have been implemented in compliance with Section C.6.14.	Select	
g) Maintain an audit trail of all changes and the associated approval.	Select		Examine a sample of change-control logs to verify that an audit trail of changes and associated approvals is maintained.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) Implement unique IDs for each administrator.	Select		Examine a sample of administrator IDs and verify that unique IDs are used.	Select	
i) Implement network device backups—e.g., system software, configuration data, and database files—prior to any change and securely store and manage all media.	Select		Examine change-control documentation to verify there is a process for backing up network devices prior to any changes to those devices. Examine procedures for backups and managing backup media to verify media are securely stored and managed. Observe the media storage location to verify it provides a secure storage environment.	Select	
j) Implement a mechanism to ensure that only authorized changes are made to network devices.	Select		Examine network device change logs to verify that changes to network devices were authorized before implementation.	Select	
C.5.4 Firewalls *The requirements in this section apply to firewalls protecting the security system networks.*					
C.5.4.1 General					
The vendor must:					
a) Ensure all documents relating to firewall configurations are stored securely.	Select		Observe the firewall configuration documentation storage area to verify: • Hard copy and non-digital documentation are stored in locked/secured areas with access only to authorized personnel. • Digital records are stored in a secure directory with access limited to authorized personnel.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Deploy an external firewall outside the SOC to protect the SOC's DMZ.	Select		Examine network diagrams and other relevant materials to verify that an external firewall outside the SOC is implemented to protect the SOC's DMZ in accordance with acceptable configurations. Examine firewall rules to verify that an external firewall is in place outside the SOC to protect the SOC's DMZ.	Select	
c) Install a firewall between the managed vendor facility security system network and the SOC network.	Select		Examine firewall rules to verify the separation via a firewall between the managed vendor facility security system network and the SOC network.	Select	
d) Deploy a physically separate firewall between the external network and the SOC DMZ and between the DMZ and the SOC network.	Select		Examine network diagrams and firewall rules to verify that firewalls are installed between the external network and the SOC DMZ and between the DMZ and the SOC network.	Select	
e) Have the capability to detect, isolate, and correct abnormal operations on network systems on a real-time basis, 24/7, on the external (DMZ) facing firewall.	Select		Examine documentation to verify that abnormal operations on network systems can be: • Detected, • Isolated, and • Corrected on a real-time, 24/7, basis. Examine a sample of logs to verify that abnormal operations on network systems are: • Detected, • Isolated, and • Corrected on a real-time, 24/7, basis.	Select	
f) Implement appropriate operating-system controls on firewalls.	Select		Examine configurations to verify that appropriate operating-system controls are implemented on firewalls.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) Review firewall rule sets and validate supporting business justification either monthly, or quarterly, with review after every firewall configuration change.	Select		Examine evidence that firewall rule sets have been validated either: • Monthly, or • After every firewall configuration change and every 3 months Examine a sample of firewall rule sets to verify that their business justification is documented.	Select	
h) Restrict physical and logical access to firewalls to only those designated personnel who are authorized to perform firewall or router administration activities.	Select		Observe the firewall/router environment to verify that that physical access to firewalls is limited to only those designated personnel who are authorized to perform administration activities. Examine a sample of access rules to verify logical access is restricted to only those designated personnel who are authorized to perform firewall or router administration activities.	Select	
i) Ensure that only authorized individuals can perform firewall administration.	Select		Examine policies and procedures to verify that only authorized individuals can perform firewall administration. Interview personnel to verify firewall administration is restricted to authorized individuals. Examine a sample of access rules to verify that only authorized individuals can perform firewall administration.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
j) Run firewalls and routers on dedicated hardware. All non-firewall-related software such as compilers, editors, and communication software must be deleted or disabled.	Select		Examine documentation to verify that non-firewall related software is deleted or disabled from firewalls and routers. Examine a sample of firewalls and routers to verify they are dedicated hardware from which all non-firewall related software has been deleted or disabled.	Select	
k) Implement daily, automated analysis reports to monitor firewall activity.	Select		Examine evidence that automated tools exist to monitor and analyze firewall activity. Observe a sample of firewall analysis reports to verify that automated analysis is in place and that daily reports are produced.	Select	
l) Use unique administrator passwords for firewalls used by the both the security system and other network devices in the facility.	Select		Examine authentication policies and procedures to verify passwords for firewall administration are different than passwords used for other network devices. Interview personnel to verify that unique passwords are established for firewall administration.	Select	
m) Implement mechanisms to protect firewall and router system logs from tampering and to check the system integrity monthly.	Select		Examine evidence that firewall and router system logs are protected from modification and a mechanism is in place to check their integrity monthly.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
n) Explicitly permit inbound and outbound traffic to the security system networks. A rule must be in place to deny all other traffic.	Select		Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the security system networks. Examine a sample of firewall and router configurations to verify that: • Approved inbound and outbound traffic for security system networks is explicitly permitted; and • All other inbound and outbound traffic is specifically denied—for example by using an explicit "deny all" or an implicit "deny after allow" statement.	Select	
C.5.4.2 Configuration					
The firewalls must:					
a) Be configured to permit network access to required services only.	Select		Examine policies and procedures for permitting network access to only required services. Examine a sample of system configuration settings to verify that the configurations permit network access to only required services.	Select	
b) Be hardened in accordance with industry best practices if the firewall is implemented on a commercial off-the-shelf (COTS) operating system.	Select		Examine policies and procedures for hardening firewalls in accordance with industry best practices. Examine a sample of firewall configuration files to verify the configurations are consistent with industry-accepted hardening standards.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Prohibit direct public access between any external networks and any system component that handles/stores security system data.	Select		Examine policies and procedures for prohibiting direct public access between any external networks and any system component that stores cardholder data to verify existence. Examine a sample of firewall and router configurations to verify there is no direct access between the Internet and system components that store cardholder data.	Select	
d) Implement IP masquerading or Network Address Translation (NAT) on the firewall between the DMZ and security system networks.	Select		Examine policies and procedures for implementing IP masquerading or Network Address Translation (NAT) on the firewall between the DMZ and the security system networks to verify existence. Examine a sample of firewall and router configurations to verify that methods are in place on the firewall between the DMZ and the security system networks to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	Select	
e) If managed remotely, be managed according to Section 4.6, "Remote Access," of the PCI CPP Logical Security Requirements.	Select		If firewalls are managed remotely, examine policy and procedures documentation to verify management activities are managed according to Section 4.6 of the PCI CPP Logical Security Requirements.	Select	
f) Be configured to deny all services not expressly permitted.	Select		Observe a sample of configuration settings to verify that all services not expressly permitted default to "deny."	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) Disable all unnecessary services, protocols, and ports. Authorized services must be documented with a business justification and be approved by the IT security manager.	Select		Interview personnel to identify necessary services, protocols, and ports. Examine a sample of systems/networks to verify that unnecessary services are disabled. Examine a sample of services, protocols, and ports to verify that their business justification is documented, and they were approved by the IT security manager.	Select	
h) Disable source routing on the firewall.	Select		Examine a sample of firewall configurations to verify that source routing is disabled.	Select	
i) Notify the administrator in real time of any items requiring immediate attention.	Select		Examine policy and procedures to verify that administrator(s) are to be notified in real time of any items requiring immediate attention. Interview administrators to verify that administrator(s) are notified in real time and that immediate attention is given when required.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
j) Maintain documented baseline security configuration standards for system components based on industry-accepted system hardening standards, which include, but are not limited to: • Center for Internet Security (CIS). • International Organization for Standardization (ISO). • SysAdmin Audit Network Security (SANS) Institute. • National Institute of Standards Technology (NIST). • At a minimum, baseline configuration must address: • User and group access security • File and directory security • Restricted services • System update and installation standards • Installed security software	Select		Examine policies and procedures to verify that a baseline configuration has been established for the organization's system components and addresses at a minimum, but not limited to: • User and group access security • File and directory security • Restricted services • System update and installation standards • Installed security software Interview personnel to verify the baseline configuration standard is based on an industry standard.	Select	
k) The vendor must perform baseline security configuration checks in the SOC environment monthly or quarterly, with review after every configuration change.	Select		Examine evidence to verify that the baseline security configuration was validated either: • Monthly, or • Quarterly with review after each configuration change. Examine a sample of baseline configuration checks to verify that they occurred either: • Monthly, or • Quarterly with review after each configuration change.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.5.5 Anti-virus Software or Programs					
The vendor must:					
a) Define, document, and follow procedures to demonstrate: • Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT). • Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components. • Inventory of current systems in the environment including information about installed software components and running services.	Select		Examine policies and procedures documentation to verify coverage of: • Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT) • Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components • Inventory of current systems in the environment including information about installed software components and about running services Interview personnel to ensure procedures are known and followed.	Select	
b) Deploy anti-virus software on all systems potentially affected by malicious software—e.g., personal computers and servers.	Select		Examine a sample of system components potentially affected by malicious software to verify that anti-virus software is deployed.	Select	
c) Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	Select		Examine a sample of system components to verify that: • Anti-virus software is present and running. • Activity logs are generated.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Check for anti-virus updates at least daily and install updates in a manner consistent with Patch Management. Documentation must show why any updates were not installed.	Select		Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date. Examine a sample of systems to verify that either updates (based upon alerts collected as part of 6.6.1.a) were applied or documentation exists for why they were not.	Select	
C.5.6 Remote Management *This section defines the remote connectivity of the managed vendor facility, the SOC, and third-party hosted locations.*					
C.5.6.1 Remote Connection Methods					
a) A managed vendor facility security system can only be connected to the SOC. ***Note:*** *A managed vendor facility is not permitted to be connected to the security system of another managed vendor facility.*	Select		Examine network topology diagrams to verify that only a managed vendor facility can be connected to the SOC	Select	
b) Event Monitoring: • Where a SOC is used for Event Monitoring, the SOC will be connected to the managed vendor facility security system and where applicable, to another SOC or SOCs of the same operational type using HTTPS/TLS secure communications. • System administration of the managed vendor facility's security system is not permitted over this type of remote connection.	Select		Examine policies and procedures to verify that remote access is NOT permitted for the administration of the managed vendor facility's security system.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Administration Services: • Administration Services can be managed from a SOC or a location that meets the requirements of a Security Control Room (SCR). The location will be connected to the individual managed vendor facility security system and, where applicable, to another SOC or SOCs of the same operational type using VPN secure communications. • Remote access for Administration Services must use a VPN that meets the requirements of Section C.6.7.3, "Virtual Private Network (VPN)."	Select		Examine policies and procedures to verify that Administration Services are only managed from a SOC or a location that meets the requirements of an SCR. Examine policies and procedures to verify that connections from the SOC to another SOC or managed vendor facility security system are done using a VPN meeting the requirements of Section C.6.7.3 (VPN)	Select	
d) Where a SOC is used for both monitoring and administration services, the services must be segregated using dedicated hardware to ensure there is no possibility of incorrect access.	Select		Examine policies and procedures to verify that if a SOC is used for both monitoring and administration services, the services are segregated using dedicated hardware to ensure there is no possibility of incorrect access.	Select	
e) External third parties must not have access for purposes other than read-only system data on live monitoring systems.	Select		Ensure policies and procedures to verify that external third parties do not have access to live monitoring systems other than read-only.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.5.6.2 Remote Connection Conditions					
a) Remote access is permitted only for the administration services of the network or system components.	Select		Examine policies and procedures to verify that remote access is permitted only for the administration of the network or system components. Examine a sample of users with remote access to verify such access is permitted only for the administration of the network or system components.	Select	
b) Remote access for administration services is permitted only from pre-determined and authorized locations using vendor-approved systems.	Select		Examine a sample of remote access system configurations and access logs to verify access is accepted only from pre-determined and authorized locations using vendor-approved systems.	Select	
c) Access using personally owned hardware is prohibited.	Select		Examine policies and procedures to verify that remote access using a personally owned device is prohibited. Examine a sample of remote access system configurations and access logs to verify that remote access from personally owned devices is not permitted.	Select	
d) Remote access is not permitted where qualified personnel are temporarily off-site and remote access is a convenience.	Select		Examine policies and procedures to verify that remote access is not permitted when qualified personnel are temporarily off-site.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) The remote access process must be fully documented and include at least the following components: • System components for which remote access is permitted. • The location from which remote access is permitted. • The conditions under which remote access is acceptable. • Users with remote access permission. • The access privileges applicable to each authorized user.	Select		Examine policies and procedures to verify the remote access process is fully documented and includes the following components but is not limited to: • System components for which remote access is permitted. • The location from which remote access is permitted. • The conditions under which remote access is acceptable. • Users with remote access permission. • The access privileges applicable to each authorized user.	Select	
f) All access privileges must be validated on a quarterly basis by an authorized individual.	Select		Examine documentation from a sample of reviews to verify that remote access privileges are reviewed at least quarterly by an authorized individual.	Select	
g) The vendor must:			Examine policies and procedures to verify the following, at a minimum:		
i. Ensure that systems allowing remote connections accept connections only from preauthorized source systems.	Select		Remote administration is predefined and preauthorized by the vendor.	Select	
ii. Ensure remote administration is predefined and preauthorized by the vendor.	Select		Remote administration is predefined and preauthorized by the vendor.	Select	
iii. Ensure remote changes comply with change-management requirements as outlined in Section C.6.13, “Change Management.”	Select		Remote changes comply with change-management requirements as outlined in Section C.6.13, “Change Management.”	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
iv. Ensure that all remote access locations are included in the facility assessment and meet these requirements.	Select		All remote access locations are included in the facility's compliance assessment and meet these requirements.	Select	
v. Be able to provide evidence of compliance validation for any remote access location.	Select		The vendor is able to provide evidence of compliance validation for any remote access location.	Select	
vi. Ensure that non-vendor staff performing remote administration maintains liability insurance to cover potential losses. All personnel performing remote administration must meet the same pre-screening qualification requirements as employees working in high-security areas.	Select		Interview a sample of non-vendor staff performing remote administration and verify that they maintain liability insurance to cover potential losses. Examine policies and procedures to verify that personnel performing remote administration must meet the same pre-screening qualification requirements as employees working in high security areas.	Select	
vii. All remote access must use a VPN that meets the requirements in the following section.	Select		Examine a sample of remote access to verify that remote access occurs using a VPN that meets the requirements of Section 6.7.3, "Virtual Private Network (VPN)."	Select	
C.5.6.3 Virtual Private Network (VPN)					
a) For remote access, VPNs must start from the originating device—e.g., PC or off-the-shelf device specifically designed for secure remote access—and terminate at either the target device or the SOC firewall. If the termination point is the firewall, it must use IPSec or at least a TLS connection in accordance with PCI DSS Requirement 4.1 to the target device.	Select		Examine VPN system documentation and a sample of configuration settings to verify that: • For remote access, VPNs must start from the originating device and terminate at either the target device or the SOC firewall. • When terminating at the SOC firewall, an IPSec or TLS connection to the target device is used in accordance with PCI Data Security Requirement 4.1.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) For remote access to DMZ components, the VPN must terminate at the target device.	Select		Examine policy and procedure documentation to verify that it defines that VPN tunnels for remote access to DMZ components must terminate at the target device.	Select	
c) SSL and TLS 1.0/1.1 are expressly prohibited in connection with the aforementioned.	Select		Examine a sample of system configurations to verify that for remote access to DMZ components, SSL and TLS 1.0/1.1 are disabled.	Select	
d) Traffic on the VPN must be encrypted using Triple DES with at least double-length keys or Advanced Encryption Standard (AES).	Select		Examine a sample of system configurations to verify that only the listed algorithms are implemented	Select	
e) Modifications to the VPN must be in compliance with the change-management requirements as outlined in Section C.6.13, "Change Management."	Select		Examine a sample of modifications made to VPN configurations and verify that changes are in compliance with the change-management requirements as outlined in Section C.6.13, "Change Management."	Select	
f) Mechanisms—e.g., digital signatures, checksums—must exist to detect unauthorized changes to VPN configuration and change-control settings.	Select		Examine a sample of VPN configuration files and change-control settings to verify they are protected from unauthorized modifications using mechanisms such as digital signatures and checksums.	Select	
g) Multi-factor authentication must be used for all VPN connections.	Select		Examine a sample of VPN system documentation and configuration settings to verify multi-factor authentication is used for VPN connections. Observe a sample of VPN access processes to verify multi-factor authentication is used.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) Access must be declined after three consecutive unsuccessful access attempts.	Select		Examine a sample of system component configuration setting to verify that authentication parameters are set to require that user accounts be locked out after not more than three consecutive invalid logon attempts.	Select	
i) Access counters may only be reset by an authorized individual after user validation by another authorized individual.	Select		Examine documentation for access counter resets to verify that it is only reset by an authorized individual after user validation by another authorized individual.	Select	
j) The connection must time out within five minutes if the session is inactive.	Select		Examine a sample of system component configuration settings to verify that system/session idle time-out features have been set to five minutes or less.	Select	
k) Remote access must be logged, and the log must be reviewed weekly for suspicious activity. Evidence of log review must be maintained.	Select		Examine documented procedures to verify remote access logs are reviewed at least weekly to identify suspicious activity and that evidence of log review is retained. Examine a sample of system configurations and audit logs to verify that remote access is logged, and that logs are reviewed.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
l) VPN traffic using Internet Protocol Security (IPSec) must meet the following additional requirements: • Tunnel mode must be used except where communication is host-to-host. • Aggressive mode must not be used for tunnel establishment. • The device authentication method must use certificates obtained from a trusted Certificate Authority. • Encapsulating Security Payload (ESP) must be used to provide data confidentiality and authentication. • The Perfect Forward Secrecy (PFS) option of Internet Key Exchange (IKE) must be used to protect against session key compromise.	Select		Examine a sample of VPN configuration files to verify that the following requirements, at a minimum, are met: • Tunnel mode must be used except where communication is host-to-host. • Aggressive mode must not be used for tunnel establishment. • The device authentication method must use certificates obtained from a trusted Certificate Authority. • Encapsulating Security Payload (ESP) must be used to provide data confidentiality and authentication. • The Perfect Forward Secrecy (PFS) option of Internet Key Exchange (IKE) must be used to protect against session key compromise.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.5.7 IT Infrastructure Requirements *The following defines the different IT infrastructure types that can be used for the SOC environment, whether internal to a certified location or using an external third-party hosting service provider. Each type has specific criteria to follow to ensure appropriate levels of security are achieved.*					
C.5.7.1 PCI CP Certified Vendor Location, external to the SOC					
a) IT Equipment that manages the SOC must be: • Housed within a facility certified to the PCI Card Production and Provisioning Standard. • Housed within a location that meets the requirements defined for a Security Control Room within the PCI Card Production and Provisioning Physical Security Requirements.	Select		Examine documentation to verify that IT Equipment that manages the SOC is: • Housed within a facility certified to the PCI Card Production and Provisioning Standard and is housed within a location that meets the requirements defined for a Security Control Room within the PCI Card Production and Provisioning Physical Security Requirements. Observe to verify that IT Equipment that manages the SOC is: • Housed within a facility certified to the PCI Card Production and Provisioning Standard. • Housed within a location that meets the requirements defined for a Security Control Room within the PCI Card Production and Provisioning Physical Security Requirements.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.5.7.2 PCI CP Certified Vendor Location, internal to the SOC					
a) IT Equipment that manages the SOC must be: • Housed within the SOC. • Housed in a separated room under access control. • Monitored by CCTV surveillance.	Select		Examine documentation to verify that IT Equipment that manages the SOC is: • Housed within the SOC • Housed in a separated room under access control • Monitored by CCTV surveillance Observe to verify that IT Equipment that manages the SOC is: • Housed within the SOC • Housed in a separated room under access control • Monitored by CCTV surveillance	Select	
C.5.8 Wireless Networks					
C.5.8.1 General					
The vendor must:					
a) Implement a documented policy regarding wireless communications and clearly communicate this policy to all employees.	Select		Examine usage policies to verify that they address wireless communications. Interview a sample of personnel and validate that the policy is clearly communicated to all card production staff.	Select	
b) Identify, analyze, and document all connections. Analysis must include purpose, risk assessment, and action to be taken.	Select		Examine a sample of connections to verify that connections are identified, analyzed, and documented including purpose, risk assessment, and action to be taken.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Use a wireless intrusion-detection system (WIDS) capable of detecting hidden and spoofed networks for all authorized wireless networks.	Select		Examine output from recent wireless scans to verify that, at a minimum: • The scan is performed for all wireless networks. • Hidden and spoofed networks can be detected.	Select	
d) When using a wireless network, use the WIDS to conduct random scans within the SOC environments at least monthly to detect rogue and hidden wireless networks.	Select		Examine output from recent wireless scans to verify that the WIDS is used to conduct random scans within the SOC environment at least monthly to detect rogue and hidden wireless networks.	Select	
e) Document, investigate, and take action to resolve any issues identified when unauthorized connections or possible intrusions are detected. The investigation must occur immediately. Resolution must occur in a timely manner.	Select		Examine policies and procedures for resolving any issues identified when unauthorized connections or possible intrusions are detected to verify existence, including that investigations must occur immediately and resolutions occur in a timely manner. Examine output from recent scan reports and verify that all unauthorized connections or possible intrusions are detected, investigated immediately, and resolved in a timely manner.	Select	
f) Use a scanning device that is capable of detecting rogue and hidden wireless networks, regardless of whether or not the vendor uses a wireless network. Random scans of the SOC environments must be conducted at least monthly.	Select		Examine policies and procedures to verify that a scanning device is used for rogue and hidden wireless networks—regardless of whether or not the vendor uses a wireless network—and that random scans of the SOC environment occur at least monthly. Examine a sample of output from recent scans to verify that the scanning device is used to conduct random scans of the SOC environment at least monthly.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.5.8.2 Additional Requirements for Using Wi-Fi					
If the wireless network uses Wi-Fi based on IEEE 802.11, the vendor must ensure that the following requirements are met:					
a) Default SSID must be changed upon installation and must be at least 8 characters.	Select		Examine vendor documentation to verify that default SSIDs are not used and new passwords are at least 8 characters. Observe a sample via using the system administrator's help to verify that default SSIDs have been changed and the new passwords are at least 8 characters.	Select	
b) A log of media access-control addresses and associated devices (including make, model, owner, and reason for access) must be maintained, and a check of authorized media access-control addresses on the access point (AP) must be conducted at least quarterly.	Select		Examine a sample of logs of media access-control addresses and associated devices to verify they include at least the make, model, owner, and reason for access. Interview personnel to verify that a check of authorized media access-control addresses on the access point (AP) is conducted at least quarterly. Examine a sample of scan reports and verify that checks of authorized media access-control addresses on the access point (AP) occur at least quarterly.	Select	
c) A media access control address-based access-control list (ACL) must be used for access control of clients.	Select		Interview responsible personnel to verify the use of ACLs for access control of clients Examine supporting documentation to verify a media access control address-based access-control list (ACL) is used for access control of clients.	Select	
d) Wi-Fi Protected Access (WPA) must be enabled if the wireless system is WPA-capable.	Select		Examine a sample of configurations and scan reports to verify that, where capable, Wi-Fi Protected Access (WPA) is enabled.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Default passwords on the AP must be changed.	Select		Examine supporting documentation to verify that default passwords on the AP are required to be changed upon installation. Observe a sample via the system administrator's help to verify that default passwords on the AP are changed.	Select	
f) The management feature for the AP must be disabled on the wireless interface and must only be managed via the trusted, wired interface.	Select		Examine configurations and verify that the management feature for the access point is disabled on the wireless interface and can only be managed via the trusted, wired interface.	Select	
g) The AP must be assigned unique Internet protocol (IP) addresses instead of relying on Dynamic Host.	Select		Examine configurations and verify that an access point is assigned unique Internet protocol (IP) addresses instead of relying on Dynamic Host.	Select	
C.5.9 Media Handling					
a) The vendor must have a documented removable-media policy that includes laptops, mobile devices, and removable storage devices—e.g., USB devices, tapes, and disks.	Select		Examine the vendor's policies and procedures for removable media documentation to verify it exists and includes devices such as laptops, mobile devices, USB devices, tapes, and disks.	Select	
b) All removable media—e.g., USB devices, tapes, disks—within the SOC must be clearly labelled with a unique identifier and the data classification.	Select		Observe a sample of removable media within the HSA to verify it is clearly labeled with a unique identifier and data classification.	Select	
c) All removable media must be securely stored, controlled, and tracked.	Select		Observe the removable media storage location to verify the area is secure. Examine the removable media check-in/out process to verify an audit trail is maintained and that it provides an accurate record of media possession.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) All removable media within the SOC must be in the custody of an authorized individual, and that individual must not have the ability to decrypt any sensitive or confidential data contained within that media.	Select		Examine a sample of checked-out, removable media within the HSA or the cloud-based provisioning environment to verify: • The media is in the custody of the person to whom the media was issued. • The individual is authorized to possess the media. • That individual does not have the ability to decrypt any sensitive or confidential data contained on that media other than in compliance with procedures for handling sensitive or confidential data. • The media does not contain clear-text confidential data.	Select	
e) A log must be maintained when media is removed from or returned to its storage location or transferred to the custody of another individual. The log must contain: • Unique identifier • Date and time • Name and signature of current custodian • Name and signature of recipient custodian • Reason for transfer	Select		Examine the media audit trail documentation to verify that it contains at least the following data points. • Unique media identifier • Date and time logged out and returned • Name and signature of the current custodian • Name and signature of custodian recipient • Reason for transfer	Select	
f) Transfers of custody between two individuals must be authorized and logged.	Select		Examine evidence that any transfer of checked out media is authorized and logged.	Select	
g) Transfer of removable media to and from the SOC must be authorized and logged.	Select		Examine a sample of media that was removed from the HSA to verify that the removal was authorized and logged.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) Physically destroy any media containing secret or confidential data when it is not possible to delete the data so that it is no longer recoverable.	Select		Examine evidence that media containing secret or confidential media is destroyed in a manner that makes it impossible to recover the data.	Select	
C.5.10 Security Testing and Monitoring					
C.5.10.1 Vulnerability					
The vendor must:					
a) Perform quarterly external network vulnerability scans using an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).	Select		Examine policies and procedures to verify that quarterly external network vulnerability scans using an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC) are required. Examine a sample of external vulnerability scans and verify that quarterly external vulnerability scans occurred in the most recent 12-month period and were completed by a PCI SSC Approved Scanning Vendor (ASV).	Select	
b) Perform internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system-component installations, changes in network topology, firewall-rule modifications, product upgrades). Scans after changes may be performed by internal staff.	Select		Examine policies and procedures to verify that internal and external network vulnerability scans are required at least quarterly and after any significant change in the network. Examine a sample (including the most recent significant change in the network) of internal and external network vulnerability scans to verify scans occur at least quarterly and after any significant change in the network.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Ensure all findings from network vulnerability scans are prioritized and tracked. Corrective action for high-priority vulnerabilities must be started within two working days.	Select		Interview responsible personnel to verify that all findings from network vulnerability scans are prioritized and tracked, and corrective action for high-priority vulnerabilities is started within two working days. Examine a sample of documentation to verify that findings from network vulnerability scans are prioritized and tracked, and corrective action for high-priority vulnerabilities is started within two working days.	Select	
d) Retain evidence of successful remediation and make this evidence available during site compliance evaluations upon request.	Select		Interview responsible personnel to verify evidence of successful remediation is retained and available upon request.	Select	
C.5.10.2 Penetration					
The vendor must:					
a) Perform internal and external penetration tests at least once a year and after any significant infrastructure changes.	Select		Examine policies and procedures to verify that internal and external penetration tests are performed at least once a year and after any significant infrastructure changes. Examine the most recent internal and external penetration tests to verify that the following requirements, at a minimum, were met:	Select	
i. The internal penetration test must not be performed remotely.	Select		The internal penetration test was not performed remotely.	Select	
ii. Penetration tests must be performed on the network layer and include all SOC network components as well as operating systems.	Select		Penetration tests were performed on the network layer and included all personalization network components as well as operating systems.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Penetration tests must be performed on the application layer and must include: • Injection flaws—e.g., SQL injection • Buffer overflow • Insecure cryptographic storage • Improper error handling • All other discovered network vulnerabilities	Select		Penetration tests were performed on the application layer and included at least the following: • Injection flaws—e.g., SQL injection • Buffer overflow • Insecure cryptographic storage • Improper error handling • Insecure communications • All other discovered high-risk network vulnerabilities	Select	
c) Ensure all findings from penetration tests are prioritized and tracked. Corrective action for high-priority vulnerabilities must be started within two working days.	Select		Interview responsible personnel to verify that all findings from penetration tests are prioritized and tracked; and corrective action for high-priority vulnerabilities is started within two working days. Examine a sample of documentation to verify that findings from penetration tests are prioritized and tracked; and corrective action for high-priority vulnerabilities is started within two working days.	Select	
d) Retain evidence of successful remediation and make this evidence available during site compliance evaluations upon request.	Select		Interview responsible personnel to verify evidence of successful remediation is retained and available upon request.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.5.11 Intrusion-Detection Systems					
The vendor must:					
a) Use intrusion-detection systems (IDS) for network traffic analysis. IDS may be implemented as part of an intrusion-prevention system (IPS) if an IPS is used. These must be deployed, managed, and maintained across the vendor networks not only for intrusion detection and prevention but also to monitor all SOC network traffic.	Select		Examine policies and procedures to verify that intrusion-detection systems are in place to monitor all traffic across the vendor networks, generated by machines within the perimeter, all SOC network traffic. Examine a sample of system configurations and network diagrams to verify that intrusion-detection systems are in place to monitor all traffic across the vendor networks, generated by machines within the perimeter, all SOC network traffic.	Select	
b) Ensure the IDS alerts personnel to suspicious activity in real time.	Select		Interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises in real time. Examine a sample of records to verify the IDS alerts personnel to suspicious activity in real time.	Select	
c) Ensure the IDS monitors all traffic at the SOC network perimeter as well as at critical points inside the SOC network.	Select		Examine system configurations and network diagrams to verify that intrusion-detection systems are in place to monitor all traffic: • At the perimeter of the SOC network • At critical points inside the SOC network	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.5.12 Change Management					
The vendor must:					
a) Ensure that change-control procedures address, at a minimum: • That requests for changes are submitted by authorized users. • Identification of components that will be changed. • Documentation of impact and back-out procedures. • Attestation of successful testing, when required. • Maintenance of an audit trail of all change requests. • Record of whether or not change was successful.	Select		Examine change-control policies and procedures to verify the following are defined: • Ensuring that requests for changes are submitted by authorized users • Identification of components that will be changed • Documentation of impact and back-out procedures • Attestation of successful testing, when required • Maintenance of an audit trail of all change requests • Record of whether or not the change was successful	Select	
b) Ensure that network and system changes follow a documented change-management process and the process is validated at least every 12 months.	Select		Examine a sample of changes to network and system components to verify changes follow the documented change-management process. Examine documentation and supporting evidence to verify that the change-management process is validated at least every 12 months.	Select	
c) Ensure all changes are approved by the CISO or authorized individual prior to deployment.	Select		Examine a sample of changes to network and system components to verify changes were approved by the CISO or authorized individual before deployment.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Ensure that the change-management process includes procedures for emergency changes.	Select		Interview personnel and review documentation to verify that the change-management process includes procedures for emergency changes. Examine a sample (if applicable) of emergency changes to verify they followed procedures.	Select	
e) Implement version identification and control for all software and documentation.	Select		Examine documentation to verify the organization's change-management policies and procedures include requirements for version control and identification.	Select	
f) Ensure that the version identification is updated when a change is released or published.	Select		Examine documentation to verify that version identification is updated when a change is released or published.	Select	
g) Implement a controlled process for the transfer of a system from test mode to live mode, and from live mode to test mode.	Select		Examine documentation to verify the existence of a controlled process for the transfer of a system from test mode to live mode, and from live mode to test mode.	Select	
h) Ensure that both development and production staff must sign off on the transfer of a system from test to live, and from live to test. This sign-off must be witnessed under dual control.	Select		Examine a sample of change-management documentation for system transfers from test to live and from live to test to verify that: • Both development and production staff sign off on the transfer of a system from test to live, and from live to test; and • This sign-off must be witnessed under dual control.	Select	
C.5.13 Configuration and Patch Management					
The vendor must:					
a) Implement a documented procedure to determine whether applicable patches and updates have become available.	Select		Examine documented procedures to verify that they include determination of whether applicable patches and updates have become available.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Make certain a process is implemented to identify and evaluate newly discovered security vulnerabilities and security patches from software vendors.	Select		Examine documentation to verify that processes are defined to identify new security vulnerabilities and obtain security patches from appropriate software vendors.	Select	
c) Ensure that secure configuration standards are established for all system components.	Select		Examine documentation to verify that secure configuration standards are established for all system components.	Select	
d) Ensure that the configuration standards include system hardening by removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Select		Examine configuration standards and verify there are requirements to remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Select	
e) Ensure that the configuration of all system components associated with data transmission, storage, and SOC activities is validated against the authorized configuration monthly.	Select		Examine documentation to verify all system components associated with data transmission, storage, and personalization are validated against the authorized configuration monthly.	Select	
f) Ensure all systems used in support of the SOC networks are actively supported in the form of regular updates.	Select		Examine documentation to verify that all systems used in support of the SOC networks are actively supported in the form of regular updates.	Select	
g) Evaluate and install the latest security-relevant patches for all system components within 30 days of their release (if they pass validation tests).	Select		Examine a sample of system components and related software to: • Compare the list of security patches installed on each system component to the most recent vendor security-patch list; and • Verify the applicable vendor-supplied security patches are installed within 30 days of their release.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) Verify the integrity and quality of the patches before application, including source authenticity.	Select		Examine procedures to verify that a process is defined, the source of the patches is authenticated, and that the quality of the patch is validated before installation. Interview personnel to verify that patch installation process conforms to written procedures.	Select	
i) Make a backup of the system being changed before applying any patches. The backup must be securely stored.	Select		Examine a sample of system components and related software and compare the list of security patches installed against backup file entries to verify backups are performed. Observe security control mechanisms for backups and verify they are in place and active. Interview personnel and review patch update procedures to verify backups are required before applying patches. Identify controls for secure storage.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
j) Implement critical patches to all Internet-facing system components within seven business days of release. When this is not possible the CISO, IT security manager, or IT director must clearly record that they understand that a critical patch is required and authorize its implementation within a maximum of 30 business days.	Select		Examine policies and procedures related to security-patch installation to verify processes are defined for installation of critical patches to Internet-facing system components within 7 business days of release. Examine a sample of Internet-facing system components and compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify that: • Applicable, critical vendor-supplied security patches are installed within 7 days of release. OR • Supporting documentation is in place recording that the CISO, IT security manager, and IT director understand and accept the risk and ensure implementation occurs within 30 business days.	Select	
k) Ensure that emergency hardware and software implementations comply with the procedures and validation requirements established for emergency implementations.	Select		Examine the documented procedures for emergency hardware and software implementation. Examine a sample of emergency and hardware and software changes to verify they follow documented procedures.	Select	
l) Ensure that emergency hardware and software implementations follow the configuration and patch management requirements in this section.	Select		Examine a sample of emergency hardware and software implementations to verify that all configuration and patch management procedures are followed. Interview personnel and review documentation to verify that emergency changes followed stated configuration and patch management requirements.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.5.14 Audit Logs					
The vendor must:					
a) Ensure that audit logs exist for all networks and network devices in the vendor environment. This includes operating system logs, security software logs, or product logs and application logs containing security events.	Select		Examine all networks and network devices in the vendor environment—including systems and applications connected to the cloud-based provision network—to ensure that audit logs are enabled and function correctly. Interview personnel to ensure that audit trails are enabled and active for identified items, including operating system logs, security software logs, product logs, and application logs containing security events.	Select	
b) Ensure that audit logs include at least the following components: • User identification • Event type • Valid date and time stamp • Success or failure indication • Origination of the event • Identity or name of the affected data, system component, or resources • Access to audit logs • Changes in access privileges	Select		Examine the audit logs to ensure they contain the required components. • User identification • Event type • Valid date and time stamp • Success or failure indication • Origination of the event • Identity or name of the affected data, system component, or resources • Access to audit logs Changes in access privileges	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Ensure that procedures are documented and followed for audit log review and reporting of unusual activity. Log reviews may be automated or manual and must include authentication, authorization, and directory servers. At a minimum, log review frequency must adhere to the following: • Immediate (real time) response to threats designated as alerts for high risk associated events • Daily review of IDS and IPS systems • Weekly review for wireless access points and authentication servers • Monthly review for routers • Monthly review of user account audit logs for databases, application, and operating systems.	Select		Examine policies and procedures to verify that procedures are defined for reviewing and reporting of unusual activity and include requirements for log frequency as stated in the requirement. Examine a sample of each log type and frequency and obtain evidence that log review was performed. Unless specified by the procedures, the order of assessment is at the discretion of the auditor. Interview personnel to verify the stated policies and procedures are known and followed.	Select	
d) Verify at least once a month that all systems are meeting log requirements.	Select		Examine evidence that demonstrates monthly verification that systems are meeting the logging requirements. Interview personnel to ensure they verify at least monthly that systems are meeting the logging requirements.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Ensure that logs for all critical systems are backed up daily, secured, and retained for at least one year. Logs must be accessible for at least three months online and one year offline.	Select		Examine logs for critical systems to: • Verify that logs are securely backed up daily. • Verify that logs are accessible online for at least three months. • Verify that logs are retained offline for one year. For both online and backed-up audit logs, review relevant security controls to ensure access is appropriate.	Select	
f) Protect and maintain the integrity of the audit logs from any form of modification.	Select		Examine relevant security controls for both online and backed-up audit logs to ensure the ability to modify or delete audit logs is prohibited.	Select	
g) Implement a security-incident and event-logging framework for its organization.	Select		Examine documentation to ensure existence of an incident-response process. interview personnel to verify they are aware of their security-incident and event-logging framework. Examine log entries to verify framework is active and in use.	Select	
C.5.15 Backup and Recovery for SOC Networks					
a) The backup and recovery procedures for SOC environments must be documented.	Select		Examine documentation to verify existence of procedures supporting the backup and recovery of the SOC environments must be documented.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) The procedures must include the backup and recovery of hardware and software that support the SOC activity.	Select		Examine documented procedures to verify they include requirements for the backup and recovery of hardware and software that support the SOC activity.	Select	
c) The procedures must differentiate between and address short-term and long-term service outages.	Select		Examine documented procedures to verify they include requirements for both short-term and long-term service outages.	Select	
d) The vendor must protect backup copies from intentional or unintentional modifications or destruction.	Select		Examine applicable access-control lists to ensure the ability to modify or delete audit backups is prohibited.	Select	
e) Backups must be encrypted and protected equivalent to the primary data as delineated in Section 3.1, "Classifications," of the PCI CPP Logical Security Standards.	Select		Interview personnel and review documentation to identify backups and their data classification. Examine documentation about the system used to protect backups to ensure that it is protected equivalent to the primary data—e.g., including the vendor, type of system/process, and the encryption algorithms used to encrypt backups. Examine a sample of backups and verify strong cryptography, with associated key-management processes and procedures where used.	Select	
f) Controls must be established to prohibit creating unauthorized backups.	Select		Examine existing security controls to verify they prohibit the creation of unauthorized backups.	Select	

Section C.5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) If the recovery procedures include an alternate processing site, the alternate site must be VPA-approved for SOC activities before any SOC activity service may begin at the alternate site.	Select		Interview personnel and review documentation to identify alternate processing sites. Examine documentation to verify that the alternate site has been VPA-approved to perform provisioning services before the provisioning occurs.	Select	

Section C.6: Software Design and Development

Section C.6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.6.1 General					
The vendor must:					
a) Document the design, development, and maintenance processes.	Select		Examine documentation of design, development, and maintenance processes to verify existence.	Select	
b) Ensure these activities are based on industry standards and security is an integral part of the software lifecycle process. Web applications must be developed based on secure coding guidelines such as the OWASP Guide, SANS CWE Top 25, and CERT Secure Coding.	Select		Examine policies and procedures to verify that: • The software life cycle process aligns with industry standards; and • Web application development is based on recognized secure coding guidelines.	Select	
c) Document all software components for each system and describe the functionality provided.	Select		Examine documentation to verify it covers software components for each system and describes how they function.	Select	

Section C.6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Protect any software backup copies from accidental destruction.	Select		Examine a sample of backups to verify they are adequately protected from accidental destruction.	Select	
C.6.2 Design					
a) The vendor must document the flow of SMS data within the environment from the receipt/generation to end of lifecycle.	Select		Examine data-flow diagrams for SMS data within the environment from the receipt/generation to end of lifecycle. Interview personnel to verify documentation includes information to support the receipt/generation of data to the end of the lifecycle.	Select	
C.6.3 Development					
The vendor must:					
a) Ensure access to source code for applications used on the SOC network is restricted to authorized personnel only.	Select		Interview personnel to identify locations of application source code. Examine system configuration and access-control lists to identify users and processes that have access to source code components. Examine approval records to ensure access to source code was authorized.	Select	
b) Ensure separation of duties exists between the staff assigned to the development environment and those assigned to the SOC environment.	Select		Examine policies and procedures to verify a separation of duties between personnel assigned to the development/test environments and those assigned to the SOC environment. Examine access-control settings to verify that access controls are in place to enforce separation of personnel assigned to the development/test environments and the SOC environment(s).	Select	

Section C.6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Ensure that software source code is restricted to only authorized staff. Staff access of source code must follow a documented process. The authorizations and approvals must be documented.	Select		Examine system configuration and access-control lists to identify users and processes that have access to source code components. Examine documented policies and procedures for granting access to source code and verify authorizations and approvals are required. Examine a sample of access request records to verify the access followed the documented process and was authorized.	Select	
C.6.4 Software Implementation					
The vendor must:					
a) Establish and maintain a documented software release process. Quality assurance must include testing of the code for security issues prior to any software releases.	Select		Interview personnel to verify a software release process exists and is in use. Examine documentation to verify a quality assurance process is required as part of the software release process and testing of code is performed before software is released. Examine a sample of recent software updates and identify evidence to verify testing of the code was performed.	Select	

Section C.6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) For internally developed software, ensure that security testing includes verification that temporary code, hard-coded keys, and suspicious code are removed.	Select		Examine policies/procedures to identify testing processes for internally developed software. Examine documentation to verify it addresses removing temporary code, hard-coded keys, and suspicious code. Examine a sample of recent internally developed software updates and verify steps to remove temporary code, hard-coded keys, and suspicious code were performed.	Select	
c) Ensure all software implementation complies with Section C.6.13, "Change Management."	Select		Examine a sample of recent software updates to verify they comply with Section C.6.13, "Change Management."	Select	
d) Test software prior to implementation to ensure correct operation.	Select		Examine a sample of recent software updates and verify evidence exists that testing software prior to implementation was performed.	Select	
e) All testing must be done on a dedicated test environment.	Select		Interview personnel to identify the controls in place to prevent debugging in the production environment. Examine policies/procedures to verify they address prevention of debugging within production environment.	Select	
f) Test and live environments must be segregated.	Select		Examine policies and procedures to verify that test and live environments are required to be separated	Select	
g) Prevent debugging within SOC environment.	Select		Examine policies and procedures to verify that debugging is not allowed within the SOC environment.	Select	
h) Have a predefined PC device configuration for PC devices used within the SOC environment.	Select		Examine policies and procedure that specify a pre-defined PC device configuration for PC devices used within the SOC environment.	Select	

Section C.6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) Implement an approval process for all software beyond the standard PC device configuration for PC devices used within the SOC environment.	Select		Examine policies and procedures to verify that an approval process exists for any PC software installed beyond the standard configuration	Select	
j) Ensure no unauthorized software can be installed.	Select		Examine policies and procedures to verify that unauthorized software is not allowed to be installed	Select	
k) Ensure all software is transferred from development to production in accordance with the change-control process.	Select		Examine policies and procedures to verify that all software transferred from development to production is required to follow the change-control process. Examine a sample of software installs to verify they followed the change-control process.	Select	

Section C.7: User Management and System Access Control

Section C.7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.7.1 User Management					
The vendor must:					
a) Ensure that procedures are documented and followed by security personnel responsible for granting access to vendor's networks, applications, and information.	Select		Interview personnel to identify those authorized to perform and processes followed for granting access to vendor's network, applications, and information. Examine documented procedures to ensure they address granting access to vendor's networks, applications, and information. Examine a sample of recent access requests to verify they were processed by authorized personnel and in accordance with documented procedures.	Select	
b) Restrict approval and level of access to staff with documented business need before access is granted. At a minimum, documented approvals must be retained while the account is active.	Select		Examine policies/procedures to ensure they address that: • Approval and level of access must be restricted to those with a documented business need before access is granted; and Documented approvals of access in place must be retained while the account is active.	Select	
c) Restrict systems access by unique user ID to only those individuals who have a business need.	Select		Examine a sample of user accounts to verify each individual associated with a unique user ID has a documented, valid business need for the system access.	Select	

Section C.7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Only grant individuals the minimum level of access sufficient to perform their duties.	Select		Interview security administration personnel to verify access is granted based on least-privilege principles sufficient to perform their duties. Examine policies/procedures to verify they require that access be granted based on least-privilege principles sufficient to perform their duties. Examine a sample of recent access requests to verify user access is limited to least privilege and based on documented business need.	Select	
e) Make certain that systems authentication requires at least the use of a unique ID and password.	Select		Examine policies/procedures for system access to verify they require at least the use of a unique ID and password. Examine system authentication settings and verify that user IDs in the system are unique and in order to gain access, a password is required.	Select	
f) Restrict administrative access to the minimum number of individuals required for management of the system.	Select		Interview management to understand the minimum number of administrative user resources required to support the personalization environment. Examine user ID lists and security privileges to identify users with administrative access and verify the number of users with administrative access aligns with management's expectations.	Select	

Section C.7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) Ensure that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values.	Select		Examine polices/procedures to verify they require that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values. Examine a sample of system components and user ID lists to verify group, shared, and generic accounts and passwords are disabled.	Select	
h) Ensure that where generic administrative accounts cannot be disabled, these accounts are used only when unique administrator sign-on credentials are not possible and only in an emergency.	Select		Interview system administration personnel to identify existence of generic accounts and how their usage is controlled. Examine policies/procedures for the management of generic administrative accounts that cannot be disabled. Verify these accounts are used only when unique administrator sign-on credentials are not possible and only in an emergency. Examine system security event log to identify when applicable generic administrative accounts were used and verify there is supporting documentation that authorizes their use in an emergency.	Select	
i) Ensure that when generic administrative accounts are used, the password is managed under dual control where no individual has access to the full password. Each component of the password must comply with the password control requirements in Section C.6.2, “Password Control.”	Select		Interview system administration personnel to verify password-management practices require that generic administrative passwords are managed under dual control and in accordance with Section 6.2 Examine policies/procedures for the management of generic administrative account passwords and verify procedures require that such passwords be managed under dual control and in accordance with Section C.6.2, “Password Control.”	Select	

Section C.7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
j) Validate all system access at least quarterly.	Select		Interview personnel to verify system access is re-validated at least quarterly. Examine validation evidence to verify the activity is performed.	Select	
k) Revalidate employee access to any systems upon a change of duties.	Select		Interview personnel to verify any staff access is revalidated when there is a change in duties. Examine a sample of HR transfer records and verify that revalidation was performed.	Select	
l) Ensure that access controls enforce segregation of duties.	Select		Interview personnel to identify that policies/procedures support segregation of duties. See glossary definition, "Segregation of Duties," in the Security Requirements.	Select	
m) Strictly limit privileged or administrative access and ensure such access is approved by both the user's manager and the IT security manager.	Select		Interview personnel to identify controls that limit privileged or administrative access. Examine access-control settings to ensure access confirms to stated policies. Examine a sample of administrative-access requests and verify access was approved by the user's manager and IT Security Manager.	Select	
n) Establish management oversight of privileged access to ensure compliance with segregation of duties.	Select		Interview personnel to identify controls that provide oversight of privileged access and compliance with segregation of duties policies. Examine policies/procedures to verify they require oversight of privileged access that ensures compliance with segregation of duties. Examine evidence—e.g., audit logs—to verify management oversight is performed.	Select	

Section C.7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
o) Ensure that all privileged administrative access is logged and reviewed weekly.	Select		Examine policies/procedures to verify that they require weekly review of privileged administrative access. Examine evidence—e.g., access logs—to verify reviews are performed according to policies and procedures.	Select	
C.7.2 Password Control					
C.7.2.1 General					
The vendor must:					
a) Implement a policy and detailed procedures relating to the generation, use, renewal, and distribution of passwords.	Select		Examine policy and detailed procedures to identify processes for generation, use, renewal, and distribution of passwords.	Select	
b) Implement procedures for handling lost, forgotten, and compromised passwords.	Select		Examine policy and detailed procedures to identify processes for handling lost, forgotten, and compromised passwords. Interview system administrators to validate adherence to procedures.	Select	
c) Distribute password procedures and policies to all users who have access to any information or system used as part of the SOC process.	Select		Examine procedures for disseminating password procedures and policies to users with access to cardholder data or any system used as part of the personalization process. Interview a sample of user population to verify password procedures and policies were distributed.	Select	
d) Ensure that only users with administrative privileges can administer other users' passwords.	Select		Examine procedures for managing user IDs and verify that only users with administrative privileges can administer user passwords. Observe a sample of user password resets and verify only users with administrative privileges can perform a reset.	Select	

Section C.7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Not store passwords in clear text.	Select		Examine system documentation and configuration settings to verify that passwords are not stored in clear text. Examine a sample of system components and their password files to verify that passwords are unreadable during storage. Change all default passwords.	Select	
f) Change all default passwords.	Select		Examine a sample of system components and attempts to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	Select	
C.7.2.2 Characteristics and Usage					
The vendor must:					
a) Systems are configured so that newly issued and reset passwords are set to a unique value for each user.	Select		Interview personnel to verify newly issued and reset passwords are set to a unique value for each user. Examine a sample of system configuration settings to verify newly issued and reset passwords are set to a unique value for each user.	Select	
b) Newly issued passwords are changed on first use.	Select		Examine system configuration settings to verify newly issued passwords are changed on first use.	Select	
c) "First use" passwords expire if not used within 24 hours of distribution.	Select		Examine system configuration settings to verify that first-time passwords are set to expire if not used within 24 hours.	Select	

Section C.7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Systems enforce password lengths of at least 12 characters.	Select		Examine the system configuration settings for a sample of system components to verify that password parameters are set to require a minimum length of at least 12 characters.	Select	
e) Passwords consist of a combination of at least three of the following: • Upper-case letters • Lower-case letters • Numbers • Special characters	Select		Examine the system configuration settings for a sample of system components to verify that user passwords are set to require at least the following strength/complexity: • Upper-case letters • Lower-case letters • Numbers • Special characters	Select	
f) Passwords are not the same as user IDs.	Select		Examine the system configuration settings for a sample of system components to verify passwords cannot be the same as the user ID.	Select	
g) Passwords are not displayed during entry.	Select		Observe authentication procedures for entering a password and verify the password is not displayed as it is entered.	Select	
h) Passwords are encrypted during transmission and rendered unreadable when stored.	Select		Examine password configurations to verify passwords are encrypted during transmission and rendered unreadable when stored. Examine a sample of passwords in transit and in storage to verify password values are not in clear text.	Select	
i) Passwords have a maximum life not to exceed 90 days and a minimum life of at least one day.	Select		Examine the system configuration settings for a sample of system components to verify that user password parameters are set to have a maximum life of not more than 90 days and a minimum life of at least one day.	Select	

Section C.7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
j) When updating passwords, the system prevents users from using a password that is the same as one of their previous four passwords.	Select		Examine the system configuration settings for a sample of system components to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.	Select	
k) The user's identity is verified prior to resetting a user password.	Select		Interview system administration personnel to verify the user's identity is verified prior to resetting a user password. Examine password reset procedures to verify the user's identify is verified prior to resetting a user password. Observe a password reset request to verify user identify is verified.	Select	
C.7.2.3 Session Locking					
The vendor must:					
a) Enforce the locking of an inactive session within a maximum of 15 minutes. If the system does not permit session locking, the user must be logged off after the period of inactivity.	Select		Examine the system configuration settings for a sample of system components to verify that system/session inactivity time out has been set to 15 minutes or less. Observe a user session to verify the user is logged out after 15 minutes, if the system does not permit session locking.	Select	
C.7.2.4 Account Locking					
a) Accounts that have been inactive for a specified period (with a maximum of 90 days) must be removed from the system.	Select		Examine user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	Select	

Section C.7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Systems must enforce the locking of a user account after a maximum of six unsuccessful authentication attempts.	Select		Examine the system configuration settings for a sample of system components to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts.	Select	
c) Locked accounts must only be unlocked by the security administrator. Alternatively, user accounts may be unlocked via automated password reset mechanisms. Challenge questions with answers that only the individual user would know must be used. These questions must be designed such that the answers are not information that is available elsewhere in the organization, such as in the Human Resources Department.	Select		Examine documented procedures to verify that accounts can only be unlocked by either the security administrator or other authorized individual, or via an automated password reset mechanism. Interview administrators to verify that an account is unlocked only after the identity of the user is verified. Examine polices/procedures for automated password reset mechanisms to verify they require conformance to the stipulated criteria. Observe the mechanism including the challenge/response criteria, for accounts that can be unlocked via an automated reset mechanism, to verify the questions are designed as stipulated in the requirement.	Select	
d) A user's account must be locked immediately upon that user leaving the vendor's employment until it is removed.	Select		Examine policies/procedures to verify that user access is locked when the user leaves the vendor's employment. Examine a record sample of users leaving vendor employment to verify that their account(s) were locked immediately.	Select	
e) A user's account must be locked immediately if that user's password is known or suspected of being compromised.	Select		Examine policies/procedures to verify that any user account is immediately locked if the password is known or suspected of being compromised.	Select	

Section C.7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) The user account logs including, but not limited to, the following must be reviewed at least twice each month for suspect lock-out activity: • Remote access • Database • Application • OS	Select		Examine the system configuration settings and audit logs for a sample of system components to verify that lock-out activity is logged. Examine documented procedures to verify access logs are reviewed at least weekly to identify suspicious activity.	Select	

Section C.8: Continuity of Service

Section C.8 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.8.1 General Requirements					
a) The vendor must have a documented contingency plan to guarantee the continuation of service provided by the SOC and each defined managed vendor facility.	Select		Examine documentation to verify existence of a contingency plan to provide for the continuation of service provided by the SOC and each defined managed vendor facility.	Select	
b) SOC and defined managed vendor facilities data must be backed up for recovery purposes in case of critical business interruption.	Select		Examine documentation to verify that SOC and defined managed vendor facilities data must be backed up for recovery purposes in case of critical business interruption. Interview personnel to verify that data backup occurs as defined in the documentation.	Select	

Section C.8 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.8.2 SOC Infrastructure ***Note:*** *Information based on Uptime Institute definitions for "Concurrently Maintainable Site Infrastructure"*					
The SOC infrastructure must meet specific requirements to ensure an adequate level of continued service is maintained. The following points are the minimum of what is needed to provide to stable service:					
a) Each SOC supplied with at least two independent internet connections to provide suitable fail-over. This enables all local sites serviced by the SOC to maintain connectivity with the SOC.	Select		Examine documentation to verify the existence of at least two independent internet connections to provide suitable fail-over.	Select	
b) Each SOC location must have auxiliary power or battery backup system to ensure all associated equipment used by the SOC is fully supported at all times.	Select		Examine documentation to verify that each SOC location has auxiliary power or battery backup system to ensure all associated equipment used by the SOC is fully supported at all times.	Select	
c) Recovery point objectives must be defined as part of SLAs to ensure minimal data loss at SOC. Source data at local site remains under the control of current requirements.	Select		Examine documentation to verify that recovery point objectives are defined as part of SLAs to ensure minimal data loss at SOC.	Select	

Section C.8 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
C.8.3 Performance Testing					
a) Each SOC must test quarterly to ensure that the level of resilience and redundancy is of sufficient adequacy to ensure continued operation for the support of the defined managed vendor facilities. The testing must include, but not limited to: • Application performance when switched between SOCs and/or the defined managed vendor facilities. • Hardware performance to ensure appropriate levels of redundancy which minimizes impacts of SOC and/or the defined managed vendor facility operations for potential outages.	Select		Examine documentation to verify that each SOC tests quarterly to ensure that the level of resilience and redundancy is of sufficient adequacy to ensure continued operation for the support of the defined managed vendor facilities and the testing includes: • Application performance when switched between SOCs and/or the defined managed vendor facilities. • Hardware performance to ensure appropriate levels of redundancy which minimizes impacts of SOC and/or the defined managed vendor facility operations for potential outages.	Select	
b) Each SOC must undergo an annual internal review to ensure the adequacy of meeting its prescribed SLAs. The following points must be included, at a minimum, but not limited to: • Standard Operating Procedure review. • Event Matrix review to ensure correct resource level is maintained. • SOC Operational team training. • SOC Operational team performance in the event of an outage.	Select		Examine documentation to verify that each SOC undergoes an annual internal review to ensure the adequacy of meeting its prescribed SLAs that includes: • Standard Operating Procedure review. • Event Matrix review to ensure correct resource level is maintained. • SOC Operational team training. • SOC Operational team performance in the event of an outage.	Select	

Section C.8 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) For each test performed above, a report must be created which details the following points: • Scope of test (included the location tested/reviewed). • Names of all individuals who were involved in the test/review. • Date of the test/review. • Evidence of the performance of the scoped area. • List of all issues that require action.	Select		Examine documentation to verify that the SOC produces a report that details the following for this Performance Testing Section: • Scope of test (included the location tested/reviewed). • Names of all individuals who were involved in the test/review. • Date of the test/review. • Evidence of the performance of the scoped area. • List of all issues that require action.	Select	
d) Each reported issue must be categorized and suitable timescales applied, as defined in the vendor policies.	Select		Examine documentation to verify that each reported issue must be categorized and suitable timescales applied, as defined in the vendor policies.	Select	
e) The Corporate Security Director must review each report on completion.	Select		Interview personnel to verify the Corporate Security Director reviews each report upon completions.	Select	