



Payment Card Industry (PCI) Card Production and Provisioning Physical Security Requirements – Security Operations Center

Attestation of Compliance for Onsite Assessments

**For use with Card Production and Provisioning Physical Security
Requirements – Appendix C: Security Operations Center v3.0.1**

Version 3.0.1

May 2024

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the card vendor's assessment with the *Payment Card Industry Card Production and Provisioning Physical Security Requirements (PCI CPPPSR) – Appendix C: Security Operations Center*. Complete all sections: The card vendor is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Card Vendor and Card Production Security Assessor – Security Operations Center Controls (CPSA-S) Information

Part 1a. Card Production and Provisioning Organization Information

Company Name:					
DBA (doing business as):			Business Identifier:		
Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Company URL:					

Part 1b. Card Production Security Assessor Company Information (if applicable)

Company Name:					
Lead Assessor Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Postal Code:	
Company URL:					

Part 2. Executive Summary

Part 2a. Scope Verification

Type of Assessment		<input type="checkbox"/> Annual audit – no monitored sites added <input type="checkbox"/> Existing location that added monitored sites <input type="checkbox"/> Initial (new facility)				
Number of card production facilities monitored						
Location information of monitored card production facilities:						
1	Business Address:			City:		
	State/Province:		Country:		Postal Code:	
2	Business Address:			City:		
	State/Province:		Country:		Postal Code:	
3	Business Address:			City:		
	State/Province:		Country:		Postal Code:	
4	Business Address:			City:		
	State/Province:		Country:		Postal Code:	
5	Business Address:			City:		
	State/Province:		Country:		Postal Code:	
6	Business Address:			City:		
	State/Province:		Country:		Postal Code:	
7	Business Address:			City:		
	State/Province:		Country:		Postal Code:	
8	Business Address:			City:		
	State/Province:		Country:		Postal Code:	
9	Business Address:			City:		
	State/Province:		Country:		Postal Code:	
10	Business Address:			City:		
	State/Province:		Country:		Postal Code:	

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

11	Business Address:		City:		
	State/Province:		Country:		Postal Code:
12	Business Address:		City:		
	State/Province:		Country:		Postal Code:
13	Business Address:		City:		
	State/Province:		Country:		Postal Code:
14	Business Address:		City:		
	State/Province:		Country:		Postal Code:
15	Business Address:		City:		
	State/Province:		Country:		Postal Code:

Part 2b. Locations

▪ 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 remote, state the rationale:		
▪ If applicable, identify date(s) spent onsite at the entity:	Start date (yyyy/mm/dd):	
	Completion date (yyyy/mm/dd):	

Part 2. Executive Summary *(continued)*

Part 2c. Summary of Requirements Tested

For each Security Operations Center Security Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Applicable” in the ROC.

Note: *Payment brand waivers do not constitute full compliance.*

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not applicable.

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

PCI Card Production and Provisioning – Security Operations Center	Details of Requirements Assessed			
	Full	Partial	None	Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not applicable and the reason.)
Section C.1: General Requirements	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Section C.2: Physical Construction Facilities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Section C.3: Security Management System	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Section C.4: SOC Personnel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Section C.5: Data Security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Section C.6: Software Design and Development	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Section C.7: User Management and System Access Control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Section C.8: Continuity of Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:		
Were any requirements in the ROC identified as being not applicable (N/A)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI Card Production and Provisioning Physical Security Validation

Based on the results noted in the ROC dated (*completion date*), the signatories identified in Parts 3b-3c, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document as of (*date*): (**check one**):

<input type="checkbox"/>	<p>Compliant: All sections of the Security Operations Center ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby (<i>Card Production and Provisioning Vendor Company Name</i>) has demonstrated full compliance with the <i>PCI Card Production and Provisioning Physical Security Requirements</i>.</p> <p>Note: Payment brand waivers do not override reporting of non-compliance.</p>						
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI Card Production and Provisioning Security Operations Center ROC are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby (<i>Card Production and Provisioning Vendor Company Name</i>) has not demonstrated full compliance with the <i>PCI Card Production and Provisioning Security Operations Center Security Requirements</i>.</p> <p>Target Date for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>Non-Compliant due to Legal exception: One or more requirements are marked Non-Compliant as "Open" or "New" due to a legal restriction that prevents the requirement from being met. This option requires additional review from the payment brand.</p> <p>Note: Contractual obligations or legal advice are not legal restrictions. If checked, complete the following:</p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(**Check all that apply**)

<input type="checkbox"/>	The ROC was completed according to the <i>PCI Card Production and Provisioning Security Operations Center Security Requirements</i> , Version (<i>version number</i>), and was completed according to the instructions therein.
<input type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have read the <i>PCI Card Production and Provisioning Security Operations Center Security Requirements</i> and I recognize that I must maintain PCI Card Production Security Requirements compliance, as applicable to my environment, at all times.
<input type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional <i>PCI Card Production and Provisioning Security Operations Center Security Requirements</i> that apply.

Part 3b. Card Production and Provisioning Vendor Attestation

Signature of Card Production and Provisioning Vendor Executive Officer ↑

Card Production and Provisioning Vendor Executive Officer Name:

Title:

Date:

Part 3c. Security Assessor Acknowledgement (if applicable)

If a Security Assessor was involved or assisted with this assessment, describe the role performed:

Signature of Assessor ↑

Date:

Assessor Name:

Assessor Company:

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI Card Production Security Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

Security Operations Center Section	Description of Requirement	Compliant to PCI Card Vendor Security Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
C.1	General Requirements	<input type="checkbox"/>	<input type="checkbox"/>	
C.2	Physical Construction	<input type="checkbox"/>	<input type="checkbox"/>	
C.3	Security Management System	<input type="checkbox"/>	<input type="checkbox"/>	
C.4	SOC Personnel	<input type="checkbox"/>	<input type="checkbox"/>	
C.5	Data Security	<input type="checkbox"/>	<input type="checkbox"/>	
C.6	Software Design and Development	<input type="checkbox"/>	<input type="checkbox"/>	
C.7	User Management and System Access Control	<input type="checkbox"/>	<input type="checkbox"/>	
C.8	Continuity of Service	<input type="checkbox"/>	<input type="checkbox"/>	

