Payment Card Industry

Data Security Standard

Self-Assessment Questionnaire SPoC and Attestation of Compliance

For use with PCI DSS Version 4.0.1

Publication Date: October 2024

Document Changes

Date	PCI DSS Version	SAQ Revision	Description
September 2023	4.0		New Self-Assessment Questionnaire for merchants using Software-based PIN entry on COTS (SPoC) solutions. This SAQ is for use with PCI DSS v4.0.
October 2024	4.0.1		Updated to align with PCI DSS v4.0.1. For details of PCI DSS changes, see *PCI DSS Summary of Changes from PCI DSS Version 4.0 to 4.0.1.* Added ASV Resource Guide to section "Additional PCI SSC Resources."

Contents

Document Changes i

Completing the Self-Assessment Questionnaire iii

Merchant Eligibility Criteria for Self-Assessment Questionnaire SPoC iii

Defining Account Data, Cardholder Data, and Sensitive Authentication Data iv

PCI DSS Self-Assessment Completion Steps iv

Expected Testing iv

Requirement Responses v

Additional PCI SSC Resources vii

Section 1: Assessment Information 1

Section 2: Self-Assessment Questionnaire SPoC 6

Protect Account Data 6

Requirement 3: Protect Stored Account Data 6

Implement Strong Access Control Measures 9

Requirement 8: Identify Users and Authenticate Assess to System Components 9

Implement Strong Access Control Measures 10

Requirement 9: Restrict Physical Access to Cardholder Data 10

Maintain an Information Security Policy 14

Requirement 12: Support Information Security with Organizational Policies and Programs 14

Appendix A: Additional PCI DSS Requirements 18

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers 18

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections 18

Appendix A3: Designated Entities Supplemental Validation (DESV) 18

Appendix B: Compensating Controls Worksheet 19

Appendix C: Explanation of Requirements Noted as Not Applicable 20

Appendix D: Explanation of Requirements Noted as Not Tested 21

Section 3: Validation and Attestation Details 22

Completing the Self-Assessment Questionnaire

Merchant Eligibility Criteria for Self-Assessment Questionnaire SPoC

This Self-Assessment Questionnaire for Software-based PIN entry on COTS (SAQ SPoC) is for merchants using a commercial off the shelf mobile device (for example, phone or tablet) with a secure card reader that is part of a SPoC Solution included on PCI SSC's list of validated[1] Software-based PIN Entry on COTS (SPoC) Solutions.

SAQ SPoC includes only those PCI DSS requirements applicable to merchants that process account data through a Secure Card Reader-PIN (SCRP) device and accompanying commercial off-the-shelf (COTS) mobile device (for example, phone or tablet), as part of a validated[1] PCI SSC Software-based PIN on COTS (SPoC) Solution.

SAQ SPoC merchants do not have access to clear-text account data on any computer system and only enter account data via an SCRP as part of a validated[1] PCI SSC SPoC Solution, using a merchant COTS mobile device. These COTS mobile devices are general-purpose mobile devices – this means that the mobile device does not have to be used only for payment or dedicated to a payment channel.

SAQ SPoC merchants process card-present transactions (contact chip transactions, contactless transactions, and SCRP-based magnetic stripe transactions).

An exception applies for merchants using non-PTS listed Magnetic Stripe Readers (MSRs); these merchants are not eligible for this SAQ. This SAQ may be used for PTS-listed SCRPs that include MSR functionality.

This SAQ is not applicable to unattended card-present (for example, kiosks, self-checkout), mail-order/telephone order (MOTO), or e-commerce channels.

This SAQ is not applicable to service providers.

SAQ SPoC merchants confirm that, for this payment channel:

- All payment processing is only via a card-present payment channel.
- All cardholder data entry is via an SCRP that is part of a validated[1] SPoC solution approved and listed by PCI SSC;
- The only systems in the merchant's SPoC environment that store, process, or transmit account data are those used as part of the validated[1] SPoC solution approved and listed by PCI SSC;
- The merchant does not otherwise receive, transmit, or store account data electronically;
- This payment channel is not connected to any other systems/networks within the merchant environment;
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- The merchant has implemented all controls in the SPoC user guide provided by the SPoC Solution Provider.

This SAQ includes only those requirements that apply to a specific type of merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to the cardholder

[1] SPoC solutions on PCI SSC's list of SPoC Solutions with an Expired Validation are no longer considered "validated" per the SPoC Program Guide. A merchant using an expired SPoC solution should check with its acquirer or individual payment brands about acceptability of this SAQ.

data environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for the merchant's environment.

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of cardholder data and/or sensitive authentication data. Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

Refer to PCI DSS Section 2, *PCI DSS Applicability Information*, for further details.

PCI DSS Self-Assessment Completion Steps

1. Confirm by review of the eligibility criteria in this SAQ and the *Self-Assessment Questionnaire Instructions and Guidelines* document on the PCI SSC website that this is the correct SAQ for the merchant's environment.
2. Confirm that the merchant environment is properly scoped.
3. Assess the environment for compliance with PCI DSS requirements.
4. Complete all sections of this document:
   - Section 1: Assessment Information (Parts 1 & 2 of the Attestation of Compliance (AOC) – Contact Information and Executive Summary).
   - Section 2: Self-Assessment Questionnaire SPoC.
   - Section 3: Validation and Attestation Details (Parts 3 & 4 of the AOC – PCI DSS Validation and Action Plan for Non-Compliant Requirements (if Part 4 is applicable)).
5. Submit the SAQ and AOC, along with any other requested documentation—such as ASV scan reports—to the requesting organization (those organizations that manage compliance programs such as payment brands and acquirers).

Expected Testing

The instructions provided in the "Expected Testing" column are based on the testing procedures in PCI DSS and provide a high-level description of the types of testing activities that a merchant is expected to perform to verify that a requirement has been met.

The intent behind each testing method is described as follows:

- Examine: The merchant critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.

- Observe: The merchant 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, environmental conditions, and physical controls.
- Interview: The merchant 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 testing methods are intended to allow the merchant to demonstrate how it has met a requirement. The specific items to be examined or observed and personnel to be interviewed should be appropriate for both the requirement being assessed and the merchant's particular implementation.

Full details of testing procedures for each requirement can be found in PCI DSS.

Requirement Responses

For each requirement item, there is a choice of responses to indicate the merchant's status regarding that requirement. ***Only one response should be selected for each requirement item.***

A description of the meaning for each response and when to use each response is provided in the table below:

Response	When to use this response:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated.
In Place with CCW (Compensating Controls Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Controls Worksheet (CCW) in Appendix B of this SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in PCI DSS in Appendices B and C.
Not Applicable	The requirement does not apply to the merchant's environment. (See "Guidance for Not Applicable Requirements" below for examples.) All responses in this column require a supporting explanation in Appendix C of this SAQ.
Not Tested	*This response is not applicable to, and not included as an option for, this SAQ.* *This SAQ was created for a specific type of environment based on how the merchant stores, processes, and/or transmits account data and defines the specific PCI DSS requirements that apply for this environment. Consequently, all requirements in this SAQ must be tested.*
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before the merchant can confirm they are in place. Responses in this column may require the completion of Part 4, if requested by the entity to which this SAQ will be submitted. This response is also used if a requirement cannot be met due to a legal restriction. (See "Legal Exception" below for more guidance).

Guidance for Not Applicable Requirements

If any requirements do not apply to the merchant's environment, select the Not Applicable option for that specific requirement. For example, in this SAQ, requirements for securing all media with cardholder data (Requirements 9.4.1 - 9.4.6) only apply if a merchant stores paper media with cardholder data; if paper media is not stored, the merchant can select Not Applicable for those requirements.

For each response where Not Applicable is selected in this SAQ, complete *Appendix C: Explanation of Requirements Noted as Not Applicable*.

Guidance for Responding to Future Dated Requirements

In Section 2 below, each PCI DSS requirement or bullet with an extended implementation period includes the following note: "*This requirement [or bullet] is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*"

These new requirements are not required to be included in a PCI DSS assessment until the future date has passed. Prior to that future date, any requirements with an extended implementation date that have not been implemented by the merchant may be marked as Not Applicable and documented in *Appendix C: Explanation of Requirements Noted as Not Applicable*.

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, select Not in Place for that requirement and complete the relevant attestation in Section 3, Part 3 of this SAQ.

Note: *A legal exception is a legal restriction due to a local or regional law, regulation, or regulatory requirement, where meeting a PCI DSS requirement would violate that law, regulation, or regulatory requirement.*

Contractual obligations or legal advice are not legal restrictions.

Use of the Customized Approach

SAQs cannot be used to document use of the Customized Approach to meet PCI DSS requirements. For this reason, the Customized Approach Objectives are not included in SAQs. Entities wishing to validate using the Customized Approach may be able to use the PCI DSS Report on Compliance (ROC) Template to document the results of their assessment.

Use of the Customized Approach is not supported in SAQs.

The use of the customized approach may be regulated by organizations that manage compliance programs, such as payment brands and acquirers. Questions about use of a customized approach should always be referred to those organizations. This includes whether an entity that is eligible for an SAQ may instead complete a ROC to use a customized approach, and whether an entity is required to use a QSA, or may use an ISA, to complete an assessment using the customized approach. Information about the use of the Customized Approach can be found in Appendices D and E of PCI DSS.

Additional PCI SSC Resources

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided below to assist with the assessment process.

Resource	Includes:
PCI Data Security Standard Requirements and Testing Procedures (PCI DSS)	▪ Guidance on Scoping ▪ Guidance on the intent of all PCI DSS Requirements ▪ Details of testing procedures ▪ Guidance on Compensating Controls ▪ Appendix G: Glossary of Terms, Abbreviations, and Acronyms
SAQ Instructions and Guidelines	▪ Information about all SAQs and their eligibility criteria ▪ How to determine which SAQ is right for your organization
Frequently Asked Questions (FAQs)	▪ Guidance and information about SAQs
Online PCI DSS Glossary	▪ PCI DSS Terms, Abbreviations, and Acronyms
Information Supplements and Guidelines	▪ Guidance on a variety of PCI DSS topics including: – *Understanding PCI DSS Scoping and Network Segmentation* – *Third-Party Security Assurance* – *Multi-Factor Authentication Guidance* – *Best Practices for Maintaining PCI DSS Compliance*
Getting Started with PCI	▪ Resources for smaller merchants including: – *Guide to Safe Payments* – *Common Payment Systems* – *Questions to Ask Your Vendors* – *Glossary of Payment and Information Security Terms* – *PCI Firewall Basics* – *ASV Resource Guide*

These and other resources can be found on the PCI SSC website *(www.pcisecuritystandards.org)*.

Organizations are encouraged to review PCI DSS and other supporting documents before beginning an assessment.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures.* Complete all sections. The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

Part 1. Contact Information	
Part 1a. Assessed Merchant	
Company name:	
DBA (doing business as):	
Company mailing address:	
Company main website:	
Company contact name:	
Company contact title:	
Contact phone number:	
Contact e-mail address:	
Part 1b. Assessor	
Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	
Qualified Security Assessor	
Company name:	
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels:

This SAQ is only applicable to card-present payment channels. Select the box below to indicate that card-present is the only payment channel that is included in this assessment.

□ Card-present

Are any payment channels not included in this assessment? If yes, indicate which channel(s) is not included in the assessment and provide a brief explanation about why the channel was excluded.	□ Yes □ No

Note: *If the organization has a payment channel that is not covered by this SAQ, consult with the entity(ies) to which this AOC will be submitted about validation for the other channels.*

Part 2b. Description of Role with Payment Cards

For each payment channel included in this assessment as selected in Part 2a above, describe how the business stores, processes and/or transmits account data.

Channel	How Business Stores, Processes, and/or Transmits Account Data

Part 2c. Description of Payment Card Environment

Provide a ***high-level*** description of the environment covered by this assessment. ***For example:*** • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	□ Yes □ No

Part 2. Executive Summary *(continued)*

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities (for example, retail locations, corporate offices, and data centers) in scope for the PCI DSS assessment.

Facility Type	**Total number of locations** (How many locations of this type are in scope)	Location(s) of facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*

Part 2e. Validated Software-based PIN Entry on COTS (SPoC) Solution

Provide the following information regarding the validated PCI SSC SPoC solution[2] used by the merchant:

Name of SPoC Solution Provider:	
Name of SPoC Solution:	
SPoC Solution listing "Reference #":	
Listed SCRP Devices used by Merchant (click "Solution Details", and look under "SCRP Devices Supported"):	
Solution "Re-evaluation Date":	
SPoC Solution Annual Checkpoint Date:	

[2] SPoC solutions on the PCI list of SPoC Solutions with Expired Validations are no longer considered "validated" per the SPoC Program Guide. Merchants using an expired SPoC solution should check with their acquirer or individual payment brands about acceptability of this SAQ. Find PCI listed products and solutions at "Products and Solutions Listings" on the PCI SSC website (www.pcisecuritystandards.org).

Part 2. Executive Summary *(continued)*	
Part 2f. Third-Party Service Providers	
Does the merchant have relationships with one or more third-party service providers that:	
• Store, process, or transmit account data on the merchant’s behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)	□ Yes □ No
• Manage system components included in the scope of the merchant’s PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.	□ Yes □ No
• Could impact the security of the merchant’s CDE (for example, vendors providing support via remote access, and/or bespoke software developers)	□ Yes □ No

If Yes:

Name of service provider:	**Description of service(s) provided:**

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

Indicate below all responses that were selected for each PCI DSS requirement.

PCI DSS Requirement *	**Requirement Responses** *More than one response may be selected for a given requirement. Indicate all responses that apply.*			
	In Place	In Place with CCW	Not Applicable	Not in Place
Requirement 3:	□	□	□	□
Requirement 8:	□	□	□	□
Requirement 9:	□	□	□	□
Requirement 12:	□	□	□	□

** PCI DSS Requirements indicated above refer to the requirements in Section 2 of this SAQ.*

Part 2h. Eligibility to Complete SAQ SPOC

Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment channel:

□	All payment processing is only via a card-present payment channel.
□	All cardholder data entry is via an SCRP that is part of a validated SPoC solution approved and listed by PCI SSC (per Part 2e above).
□	The only systems in the merchant SPoC environment that store, process, or transmit account data are those used as part of a validated SPoC solution approved and listed by PCI SSC.
□	The merchant does not otherwise receive, transmit, or store account data electronically.
□	This payment channel is not connected to any other systems/networks within the merchant environment.
□	Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.
□	The merchant has implemented all controls in the SPoC user guide provided by the SPoC Solution Provider.

Section 2: Self-Assessment Questionnaire SPoC

Note: *The following requirements mirror the requirements in the* PCI DSS Requirements and Testing Procedures *document.*

Self-assessment completion date: YYYY-MM-DD

Protect Account Data

Requirement 3: Protect Stored Account Data

Note: *For SAQ SPoC, Requirement 3 applies only to merchants with paper records that include account data (for example, receipts or printed reports).*

PCI DSS Requirement		**Expected Testing**	**Response**♦ *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
3.1 Processes and mechanisms for protecting stored account data are defined and understood.						
3.1.1	All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	□	□	□	□
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 3.1.1 means that, if the merchant has paper storage of account data, the merchant has policies and procedures in place that govern merchant activities for Requirement 3. This helps to ensure personnel are aware of and following security policies and documented operational procedures for managing the secure storage of any paper records with account data.* *If merchant does not store paper records with account data, mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.*						

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
3.2 Storage of account data is kept to a minimum.						
3.2.1	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	• Examine the data retention and disposal policies, procedures, and processes. • Interview personnel. • Examine files and system records on system components where account data is stored. • Observe the mechanisms used to render account data unrecoverable.	□	□	□	□
	Applicability Notes					
	Where account data is stored by a TPSP (for example, in a cloud environment), entities are responsible for working with their service providers to understand how the TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a data element are securely deleted. *The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.*					

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 3.2.1 means that the merchant has data disposal policies that govern account data storage and if a merchant stores any paper (for example, receipts or paper reports) that contain account data, the merchant stores the paper per that policy (for example, only as long as it is needed for business, legal, and/or regulatory reasons) and destroys the paper once it is no longer needed.* *If a merchant never prints or stores any paper containing account data, mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.*						
3.3 Sensitive authentication data (SAD) is not stored after authorization.						
3.3.1.2	The card verification code is not stored upon completion of the authorization process.	• Examine data sources.	□	□	□	□
	Applicability Notes					
	The card verification code is the three- or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions.					
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 3.3.1.2 means that if the merchant writes down the card verification code while a transaction is being conducted, the merchant either securely destroys the paper (for example, with a shredder) immediately after the transaction is complete, or obscures the code (for example, by "blacking it out" with a marker) before the paper is stored.* *If the merchant never requests the three-digit or four-digit number printed on the front or back of a payment card ("card verification code"), mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.*						

Implement Strong Access Control Measures

Requirement 8: Identify Users and Authenticate Assess to System Components

Note: *For SAQ SPoC, Requirement 8 only applies to authentication used on the merchant's COTS device.*

PCI DSS Requirement		**Expected Testing**	**Response♦** *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
8.3 Strong authentication for users and administrators is established and managed						
8.3.1	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric element.	• Examine documentation describing the authentication factor(s) used. • For each type of authentication factor used with each type of system component, observe the authentication process.	□	□	□	□
	Applicability Notes					
	This Applicability Note was intentionally removed as it does not apply to SAQ SPoC assessments.					

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

Implement Strong Access Control Measures

Requirement 9: Restrict Physical Access to Cardholder Data

PCI DSS Requirement		Expected Testing	**Response**[♦] *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.						
9.1.1	All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	□	□	□	□
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 9.1.1 means that the merchant has policies and procedures in place that govern merchant activities for Requirement 9, including how any paper media with cardholder data is secured, and how POI devices are protected.*						
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.						
Note: *For SAQ SPoC, Requirements at 9.4 only apply to merchants with paper records (for example, receipts or printed reports) with account data, including primary account numbers (PANs).*						
9.4.1	All media with cardholder data is physically secured.	• Examine documentation.	□	□	□	□
9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	• Examine documented procedures. • Examine logs or other documentation. • Interview responsible personnel at the storge location(s).	□	□	□	□

[♦] *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.4.6	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.	• Examine the media destruction policy. • Observe processes. • Interview personnel. • Observe storage containers.	□	□	□	□
	Applicability Notes					
	These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.					

SAQ Completion Guidance:

Selection of any of the In Place responses for Requirements at 9.4 means that the merchant securely stores any paper media with account data, for example by storing the paper in a locked drawer, cabinet, or safe, and that the merchant destroys such paper when no longer needed for business purposes. This includes a written document or policy for employees, so they know how to secure paper with account data and how to destroy the paper when no longer needed.

If the merchant never stores any paper with account data, mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

PCI DSS Requirement		Expected Testing	**Response♦** *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.						
Note: *For SAQ SPoC, these requirements apply to the POI devices (for example, SCRPs) used by the merchant at part of the SPoC solution.*						
9.5.1	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	• Examine documented policies and procedures.	□	□	□	□
	Applicability Notes These requirements apply to deployed POI devices used in card-present transactions (that is, a payment card form factor such as a card that is swiped, tapped, or dipped). These requirements do not apply to: • Components used only for manual PAN key entry. • Commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution.					
9.5.1.1	An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.	• Examine the list of POI devices. • Observe POI devices and device locations. • Interview personnel.	□	□	□	□
9.5.1.2	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	• Examine documented procedures. • Interview responsible personnel. • Observe inspection processes.	□	□	□	□
9.5.1.2.1	*Requirement intentionally left blank for this SAQ.*					

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.5.1.3	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	• Review training materials for personnel in POI environments. • Interview responsible personnel.	□	□	□	□

Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

***Note:** Requirement 12 specifies that merchants have information security policies for their personnel, but these policies can be as simple or complex as needed for the size and complexity of the merchant's operations. The policy document must be provided to all personnel so they are aware of their responsibilities for protecting payment terminals, any paper documents with cardholder data and/or sensitive authentication data, etc. If a merchant has no employees, then it is expected that the merchant understands and acknowledges their responsibility for security within their store(s).*

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.						
12.1.1	An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	• Examine the information security policy. • Interview personnel.	□	□	□	□
12.1.2	The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment	• Examine the information security policy. • Interview responsible personnel.	□	□	□	□

SAQ Completion Guidance:

Selection of any of the In Place responses for Requirements 12.1.1 and 12.1.2 means that the merchant has a security policy that is reasonable for the size and complexity of the merchant's operations, and that the policy is reviewed at least once every 12 months and updated if needed. For example, such a policy could be a simple document that covers how to protect the store and payment devices in accordance with the solution provider's guidance/instruction manual, and who to call in an emergency.

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.1.3	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	• Examine the information security policy. • Interview responsible personnel. • Examine documented evidence.	□	□	□	□
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 12.1.3 means that the merchant's security policy defines basic security responsibilities for all personnel, consistent with the size and complexity of the merchant's operations. For example, security responsibilities could be defined according to basic responsibilities by employee levels, such as the responsibilities expected of a manager/owner and those expected of clerks.*						
12.6 Security awareness education is an ongoing activity.						
12.6.1	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	• Examine the security awareness program.	□	□	□	□
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 12.6.1 means that the merchant has a security awareness program in place, consistent with the size and complexity of the merchant's operations. For example, a simple awareness program could be a flyer posted in the back office, or a periodic e-mail sent to all employees. Examples of awareness program messaging include descriptions of security tips all employees should follow, such as how to lock doors and storage containers, how to determine whether a payment terminal has been tampered with, and processes to confirm the identity and verify there is a legitimate business reason for any service workers when they arrive to service payment terminals.*						
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.						
12.8.1	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	• Examine policies and procedures. • Examine list of TPSPs.	□	□	□	□
	Applicability Notes The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.					

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.8.2	Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that TPSPs are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that the TPSP could impact the security of the entity's cardholder data and/or sensitive authentication data.	• Examine policies and procedures. • Examine written agreements with TPSPs.	□	□	□	□
	Applicability Notes					
	The exact wording of an agreement will depend on the details of the service being provided, and the responsibilities assigned to each party. The agreement does not have to include the exact wording provided in this requirement. The TPSP's written acknowledgment is a confirmation that states the TPSP is responsible for the security of the account data it may store, process, or transmit on behalf of the customer or to the extent the TPSP may impact the security of a customer's cardholder data and/or sensitive authentication data. Evidence that a TPSP is meeting PCI DSS requirements (is not the same as a written acknowledgment specified in this requirement. For example, a PCI DSS Attestation of Compliance (AOC), a declaration on a company's website, a policy statement, a responsibility matrix, or other evidence not included in a written agreement is not a written acknowledgment.					
12.8.3	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	• Examine policies and procedures. • Examine evidence. • Interview responsible personnel.	□	□	□	□

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	□	□	□	□
	Applicability Notes					
	Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.					
12.8.5	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	□	□	□	□
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirements 12.8.1 through 12.8.5 means that the merchant has a list of, and agreements with, service providers they share account data with or that could impact the security of the merchant's cardholder data environment. For example, such agreements would be applicable if a merchant uses a document-retention company to store paper documents that include account data or if a merchant's vendor accesses merchant systems remotely to perform maintenance.*						
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.						
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident.	• Examine the incident response plan. • Interview personnel. • Examine documentation from previously reported incidents.	□	□	□	□
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 12.10.1 means that the merchant has documented an incident response and escalation plan to be used for emergencies, consistent with the size and complexity of the merchant's operations. For example, such a plan could be a simple document posted in the back office that lists who to call in the event of various situations with an annual review to confirm it is still accurate, but could extend all the way to a full incident response plan including backup "hotsite" facilities and thorough annual testing. This plan should be readily available to all personnel as a resource in an emergency.*						

Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

This Appendix is not used for merchant assessments.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections

This Appendix is not used for SAQ SPoC merchant assessments.

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities required to validate to this Appendix should use the DESV Supplemental Reporting Template and Supplemental Attestation of Compliance for reporting, and consult with the applicable payment brand and/or acquirer for submission procedures.

Appendix B: Compensating Controls Worksheet

This Appendix must be completed to define compensating controls for any requirement where In Place with CCW was selected.

***Note:** Only entities that have a legitimate and documented technological or business constraint can consider the use of compensating controls to achieve compliance.*

Refer to Appendices B and C in PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	Document the legitimate technical or business constraints precluding compliance with the original requirement.	
2. Definition of Compensating Controls	Define the compensating controls: explain how they address the objectives of the original control and the increased risk, if any.	
3. Objective	Define the objective of the original control.	
	Identify the objective met by the compensating control. ***Note:** This can be, but is not required to be, the stated Customized Approach Objective listed for this requirement in PCI DSS.*	
4. Identified Risk	Identify any additional risk posed by the lack of the original control.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process(es) and controls in place to maintain compensating controls.	

Appendix C: Explanation of Requirements Noted as Not Applicable

This Appendix must be completed for each requirement where Not Applicable was selected.

Requirement	Reason Requirement is Not Applicable
Example:	
Requirement 3.5.1	*Account data is never stored electronically*

Appendix D: Explanation of Requirements Noted as Not Tested

This Appendix is not used for SAQ SPoC merchant assessments.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ SPOC (Section 2), dated (Self-assessment completion date *YYYY-MM-DD).*

Based on the results documented in the SAQ SPOC noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the merchant identified in Part 2 of this document.

Select one:

<table>
<tr><td>□</td><td><b>Compliant:</b> All sections of the PCI DSS SAQ are complete and all requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>(Merchant Company Name)</i> has demonstrated compliance with all PCI DSS requirements included in this SAQ.</td></tr>
<tr><td>□</td><td><b>Non-Compliant:</b> Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall <b>NON-COMPLIANT</b> rating; thereby <i>(Merchant Company Name)</i> has not demonstrated compliance with the PCI DSS requirements included in this SAQ.
<b>Target Date</b> for Compliance: <i>YYYY-MM-DD</i>
A merchant submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted <i>before completing Part 4.</i></td></tr>
<tr><td>□</td><td><b>Compliant but with Legal exception:</b> One or more requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall <b>COMPLIANT BUT WITH LEGAL EXCEPTION</b> rating; thereby <i>(Merchant Company Name)</i> has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not in Place due to a legal restriction.
This option requires additional review from the entity to which this AOC will be submitted. <i>If selected, complete the following:</i>
<table>
<tr><th>Affected Requirement</th><th>Details of how legal constraint prevents requirement from being met</th></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>
</td></tr>
</table>

Part 3a. Merchant Acknowledgement

Signatory(s) confirms:
(Select all that apply)

□	*PCI DSS Self-Assessment Questionnaire SPOC, Version 4.0.1,* was completed according to the instructions therein.
□	All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.
□	PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer ↑	*Date: YYYY-MM-DD*
Merchant Executive Officer Name:	*Title:*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this assessment, indicate the role performed:	□ QSA performed testing procedures.
	□ QSA provided other assistance. If selected, describe all role(s) performed:

Signature of Lead QSA ↑	*Date: YYYY-MM-DD*
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date: YYYY-MM-DD*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this assessment, indicate the role performed:	□ ISA(s) performed testing procedures.
	□ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the merchant expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement *	**Description of Requirement**	**Compliant to PCI DSS Requirements** (Select One)		**Remediation Date and Actions** (If "NO" selected for any Requirement)
		YES	**NO**	
3	Protect stored account data	□	□	
8	Identify users and authenticate assess to system components.	□	□	
9	Restrict physical access to cardholder data.	□	□	
12	Support information security with organizational policies and programs	□	□	

** PCI DSS Requirements indicated above refer to the requirements in Section 2 of this SAQ.*

***Note:** The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance-accepting organization to ensure that this form is acceptable in its program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/.*