# Payment Card Industry
# Data Security Standard

## Self-Assessment Questionnaire B-IP 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 |
|---|---|---|---|
| N/A | 1.0 | | Not used. |
| N/A | 2.0 | | Not used. |
| February 2014 | 3.0 | | New SAQ to address requirements applicable to merchants who process cardholder data only via standalone, PTS-approved point-of-interaction devices with an IP connection to the payment processor.<br><br>Content aligns with PCI DSS v3.0 requirements and testing procedures. |
| April 2015 | 3.1 | | Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1.* |
| July 2015 | 3.1 | 1.1 | Updated to remove references to "best practices" prior to June 30, 2015. |
| April 2016 | 3.2 | 1.0 | Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2.*<br><br>Requirements added from PCI DSS v3.2 Appendix A2. |
| January 2017 | 3.2 | 1.1 | Updated Document Changes to clarify requirements added in the April 2016 update.<br><br>Updated Before You Begin section to clarify term "SCR" and intent of permitted systems.<br><br>Added Requirement 8.3.1 to align with intent of Requirement 2.3.<br><br>Added Requirement 11.3.4 to verify segmentation controls, if segmentation is used. |
| June 2018 | 3.2.1 | 1.0 | Updated to align with PCI DSS v3.2.1. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1.* |
| April 2022 | 4.0 | | Updated to align with PCI DSS v4.0. For details of PCI DSS changes, see PCI DSS – Summary of Changes from PCI DSS Version 3.2.1 to 4.0.<br><br>Rearranged, retitled, and expanded information in the "Completing the Self-Assessment Questionnaire" section (previously titled "Before You Begin").<br><br>Aligned content in Sections 1 and 3 of Attestation of Compliance (AOC) with PCI DSS v4.0 Report on Compliance AOC.<br><br>Added PCI DSS v4.0 requirements.<br><br>Added appendices to support new reporting responses. |
| December 2022 | 4.0 | 1 | Removed "In Place with Remediation" as a reporting option from Requirement Responses table, Attestation of Compliance (AOC) Part 2g, SAQ Section 2 Response column, and AOC Section 3. Also removed former Appendix C.<br><br>Added "In Place with CCW" to AOC Section 3.<br><br>Added guidance for responding to future-dated requirements.<br><br>Added minor clarifications and addressed typographical errors. |
| January 2024 | 4.0 | 2 | Added Requirement 4.2.1 into this SAQ. This requirement, which has been present in SAQ B-IP for previous PCI DSS versions, was inadvertently removed when this SAQ was updated for 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.*<br><br>Added ASV Resource Guide to section "Additional PCI SSC Resources." |

# Contents

## Completing the Self-Assessment Questionnaire

### Merchant Eligibility Criteria for Self-Assessment Questionnaire B-IP

Self-Assessment Questionnaire (SAQ) B-IP includes only those PCI DSS requirements applicable to merchants that process account data only via standalone, PCI-listed approved[1] PIN Transaction Security (PTS) point-of-interaction (POI) devices with an IP connection to the payment processor.

An exception applies for PTS POI devices classified as Secure Card Readers (SCR) and Secure Card Readers for PIN (SCRPs); merchants using SCRs or SCRPs are not eligible for this SAQ.

SAQ B-IP merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants, and do not store account data on any computer system.

***This SAQ is not applicable to e-commerce channels.***

***This SAQ is not applicable to service providers.***

SAQ B-IP merchants confirm that, for this payment channel:

- The merchant uses only standalone, PCI-listed approved[1] PTS POI devices (excludes SCRs and SCRPs) connected via IP to merchant's payment processor to take customers' payment card information;

- The standalone, IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs and SCRPs);

- The standalone, IP-connected PTS POI devices are not connected to any other systems within the merchant environment (this can be achieved via network segmentation to isolate PTS POI devices from other systems)[2];

- The only transmission of account data is from the approved PTS POI devices to the payment processor;

- The PTS POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor;

- The merchant does not store account data in electronic format; and

- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

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 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.

---

[1] A merchant using an expired PTS POI device should check with its acquirer or individual payment brands about acceptability of this SAQ. Refer to PCI's list of PIN Transaction Security Devices with Expired Approvals.

[2] This criteria is not intended to prohibit more than one of the permitted system type (that is, IP-connected POI devices) being on the same network zone, as long as the permitted systems are isolated from other types of systems (e.g. by implementing network segmentation). Additionally, this criteria is not intended to prevent the defined system type from being able to transmit transaction information to a third party for processing, such as an acquirer or payment processor, over a network.

## 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)<br>• Cardholder Name<br>• Expiration Date<br>• Service Code | • Full track data (magnetic-stripe data or equivalent on a chip)<br>• Card verification code<br>• 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 B-IP.

   ▪ 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** <br><br> (Compensating Controls Worksheet) | The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. <br><br> All responses in this column require completion of a Compensating Controls Worksheet (CCW) in Appendix B of this SAQ. <br><br> 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.). <br><br> 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.* <br><br> *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. <br><br> 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<br>▪ Guidance on the intent of all PCI DSS Requirements<br>▪ Details of testing procedures<br>▪ Guidance on Compensating Controls<br>▪ Appendix G: Glossary of Terms, Abbreviations, and Acronyms |
| SAQ Instructions and Guidelines | ▪ Information about all SAQs and their eligibility criteria<br>▪ 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:<br>  – *Understanding PCI DSS Scoping and Network Segmentation*<br>  – *Third-Party Security Assurance*<br>  – *Multi-Factor Authentication Guidance*<br>  – *Best Practices for Maintaining PCI DSS Compliance* |
| Getting Started with PCI | ▪ Resources for smaller merchants including:<br>  – *Guide to Safe Payments*<br>  – *Common Payment Systems*<br>  – *Questions to Ask Your Vendors*<br>  – *Glossary of Payment and Information Security Terms*<br>  – *PCI Firewall Basics*<br>  – *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 (select all that apply):

Indicate all payment channels used by the business that are included in this assessment.

☐ Mail order/telephone order (MOTO)

☐ E-Commerce

☐ Card-present

| | |
|---|---|
| Are any payment channels not included in this assessment? <br><br> 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. <br><br> *For example:* <br> • *Connections into and out of the cardholder data environment (CDE).* <br> • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* <br> • *System components that could impact the security of account data.* | |
| Indicate whether the environment includes segmentation to reduce the scope of the assessment. <br><br> *(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, data centers, call centers, and mail rooms) 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. PCI SSC Validated Products and Solutions

Does the merchant use any item identified on any PCI SSC Lists of Validated Products and Solutions♦?

☐ Yes   ☐ No

Provide the following information regarding each item the merchant uses from PCI SSC's Lists of Validated Products and Solutions.

| Name of PCI SSC validated Product or Solution | Version of Product or Solution | PCI SSC Standard to which product or solution was validated | PCI SSC listing reference number | Expiry date of listing (YYYY-MM-DD) |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

---

♦ For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions, and Mobile Payments on COTS (MPoC) products.

## 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 1: | ☐ | ☐ | ☐ | ☐ |
| Requirement 2: | ☐ | ☐ | ☐ | ☐ |
| Requirement 3: | ☐ | ☐ | ☐ | ☐ |
| Requirement 4: | ☐ | ☐ | ☐ | ☐ |
| Requirement 6: | ☐ | ☐ | ☐ | ☐ |
| Requirement 7: | ☐ | ☐ | ☐ | ☐ |
| Requirement 8: | ☐ | ☐ | ☐ | ☐ |
| Requirement 9: | ☐ | ☐ | ☐ | ☐ |
| Requirement 11: | ☐ | ☐ | ☐ | ☐ |
| Requirement 12: | ☐ | ☐ | ☐ | ☐ |
| Appendix A2: | ☐ | ☐ | ☐ | ☐ |

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

## Part 2. Executive Summary *(continued)*

### Part 2h. Eligibility to Complete SAQ B-IP

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

| | |
|---|---|
| ☐ | The merchant uses only standalone, PCI-listed approved PTS POI devices (excludes SCRs and SCRPs) connected via IP to merchant's payment processor to take customers' payment card information. |
| ☐ | The standalone IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs and SCRPs). |
| ☐ | The standalone IP-connected PTS POI devices are not connected to any other systems within the merchant environment (this can be achieved via network segmentation to isolate PTS POI devices from other systems). |
| ☐ | The only transmission of account data is from the approved PTS POI devices to the payment processor. |
| ☐ | The PTS POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor. |
| ☐ | The merchant does not store account data in electronic format. |
| ☐ | Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically. |

## Section 2: Self-Assessment Questionnaire B-IP

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

**Self-assessment completion date:** YYYY-MM-DD

## Build and Maintain a Secure Network and Systems

### *Requirement 1: Install and Maintain Network Security* Controls

| PCI DSS Requirement | Expected Testing | Response♦ *(Check one response for each requirement)* | | | |
|---|---|---|---|---|---|
| | | In Place | In Place with CCW | Not Applicable | Not in Place |
| **1.2** Network security controls (NSCs) are configured and maintained. | | | | | |
| **1.2.3** An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks. | • Examine network diagrams. <br> • Examine network configurations. <br> • Interview responsible personnel. | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes** <br><br> A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement. | | | | | |
| **1.2.5** All services, protocols and ports allowed are identified, approved, and have a defined business need. | • Examine documentation. <br> • Examine configuration settings. | ☐ | ☐ | ☐ | ☐ |
| **1.2.6** Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated. | • Examine documentation. <br> • Examine configuration settings. | ☐ | ☐ | ☐ | ☐ |

---

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

| PCI DSS Requirement | Expected Testing | Response<br>(Check one response for each requirement) | | | |
|---|---|---|---|---|---|
| | | In Place | In Place with CCW | Not Applicable | Not in Place |
| **1.3** Network access to and from the cardholder data environment is restricted. | | | | | |
| **1.3.1** Inbound traffic to the CDE is restricted as follows:<br>• To only traffic that is necessary.<br>• All other traffic is specifically denied. | • Examine NSC configuration standards.<br>• Examine NSC configurations. | ☐ | ☐ | ☐ | ☐ |
| **1.3.2** Outbound traffic from the CDE is restricted as follows:<br>• To only traffic that is necessary.<br>• All other traffic is specifically denied. | • Examine NSC configuration standards.<br>• Examine NSC configurations. | ☐ | ☐ | ☐ | ☐ |
| **1.3.3** NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that:<br>• All wireless traffic from wireless networks into the CDE is denied by default.<br>• Only wireless traffic with an authorized business purpose is allowed into the CDE. | • Examine configuration settings.<br>• Examine network diagrams. | ☐ | ☐ | ☐ | ☐ |
| **1.4** Network connections between trusted and untrusted networks are controlled. | | | | | |
| **1.4.3** Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network. | • Examine NSC documentation.<br>• Examine NSC configurations. | ☐ | ☐ | ☐ | ☐ |

## *Requirement 2: Apply Secure Configurations to All System Components*

*Note: For SAQ B-IP, Requirement 2 applies to firewall/router devices on the merchant's network that connect its PTS POI devices to the payment processor.*

| PCI DSS Requirement | Expected Testing | Response♦ (Check one response for each requirement) | | | |
|---|---|---|---|---|---|
| | | In Place | In Place with CCW | Not Applicable | Not in Place |
| **2.2** System components are configured and managed securely. | | | | | |
| **2.2.2** Vendor default accounts are managed as follows:<br>• If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.<br>• If the vendor default account(s) will not be used, the account is removed or disabled. | • Examine system configuration standards.<br>• Examine vendor documentation.<br>• Observe a system administrator logging on using vendor default accounts.<br>• Examine configuration files.<br>• Interview personnel. | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes**<br><br>This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) defaults.<br><br>This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service. | | | | | |
| **2.2.7** All non-console administrative access is encrypted using strong cryptography. | • Examine system configuration standards.<br>• Observe an administrator log on.<br>• Examine system configurations.<br>• Examine vendor documentation.<br>• Interview personnel. | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes**<br><br>This includes administrative access via browser-based interfaces and application programming interfaces (APIs). | | | | | |

---

♦ *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 |
| **2.3** Wireless environments are configured and managed securely. | | | | | |
| **2.3.1** For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to:<br>• Default wireless encryption keys.<br>• Passwords on wireless access points.<br>• SNMP defaults.<br>• Any other security-related wireless vendor defaults. | • Examine policies and procedures.<br>• Review vendor documentation.<br>• Examine wireless configuration settings.<br>• Interview personnel. | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes** | | | | | |
| This includes, but is not limited to, default wireless encryption keys, passwords on wireless access points, SNMP defaults, and any other security-related wireless vendor defaults. | | | | | |
| **2.3.2** For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows:<br>• Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary.<br>• Whenever a key is suspected of or known to be compromised. | • Examine key-management documentation.<br>• Interview personnel. | ☐ | ☐ | ☐ | ☐ |

# Protect Account Data

## Requirement 3: Protect Stored Account Data

*Note: For SAQ B-IP, 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:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | • Examine documentation.<br>• 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 |
| **3.3** Sensitive authentication data (SAD) is not stored after authorization. | | | | | |
| **3.3.1** SAD is not stored after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process. | • Examine documented policies and procedures. <br> • Examine system configurations. <br> • Observe the secure data deletion processes. | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes** <br><br> *Part of this Applicability Note was intentionally removed for this SAQ as it does not apply to merchant assessments.* <br><br> Sensitive authentication data includes the data cited in Requirements 3.3.1.1 through 3.3.1.2. | | | | | |
| **3.3.1.1** The full contents of any track are not stored upon completion of the authorization process. | • Examine data sources. | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes** <br><br> In the normal course of business, the following data elements from the track may need to be retained: <br> • Cardholder name. <br> • Primary account number (PAN). <br> • Expiration date. <br> • Service code. <br> To minimize risk, store securely only these data elements as needed for business. | | | | | |
| **3.3.1.2** The card verification code is not stored upon completion of the authorization process. | • Examine data sources. | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes** <br><br> 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. | | | | | |

| PCI DSS Requirement | Expected Testing | Response◆ *(Check one response for each requirement)* | | | |
|---|---|---|---|---|---|
| | | In Place | In Place with CCW | Not Applicable | Not in Place |

| | PCI DSS Requirement | Expected Testing | In Place | In Place with CCW | Not Applicable | Not in Place |
|---|---|---|---|---|---|---|
| **3.3.1.3** | The personal identification number (PIN) and the PIN block are not stored upon completion of the authorization process. | • Examine data sources. | ☐ | ☐ | ☐ | ☐ |

**Applicability Notes**

PIN blocks are encrypted during the natural course of transaction processes, but even if an entity encrypts the PIN block again, it is still not allowed to be stored after the completion of the authorization process.

**3.4** Access to displays of full PAN and ability to copy PAN are restricted.

| | | | In Place | In Place with CCW | Not Applicable | Not in Place |
|---|---|---|---|---|---|---|
| **3.4.1** | PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN. | • Examine documented policies and procedures.<br>• Examine system configurations.<br>• Examine the documented list of roles that need access to more than the BIN and last four digits of the PAN (includes full PAN).<br>• Examine displays of PAN (for example, on screen, on paper receipts). | ☐ | ☐ | ☐ | ☐ |

**Applicability Notes**

This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment brand requirements for point-of-sale (POS) receipts.

This requirement relates to protection of PAN where it is displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.5.1 for protection of PAN when stored, processed, or transmitted.

## Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

| PCI DSS Requirement | Expected Testing | Response♦ (Check one response for each requirement) | | | |
|---|---|---|---|---|---|
| | | In Place | In Place with CCW | Not Applicable | Not in Place |
| **4.2** PAN is protected with strong cryptography during transmission. | | | | | |
| **4.2.1** Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: | | | | | |
| • Only trusted keys and certificates are accepted. | • Examine documented policies and procedures. • Interview personnel. • Examine system configurations. • Examine cardholder data transmissions. • Examine keys and certificates. | ☐ | ☐ | ☐ | ☐ |
| • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* | | ☐ | ☐ | ☐ | ☐ |
| • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. | | ☐ | ☐ | ☐ | ☐ |
| • The encryption strength is appropriate for the encryption methodology in use. | | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes** *(continued)* | | | | | |

♦ *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 |
| **4.2.1** (cont.) | *Part of this Applicability Note was intentionally removed as it does not apply to this SAQ.*<br><br>*The bullet above (for confirming that certificates used to safeguard PAN during transmission over open, public networks are valid and are not expired or revoked) is a best practice until 31 March 2025, after which it will be required as part of Requirement 4.2.1 and must be fully considered during a PCI DSS assessment.* | | | | | |

*SAQ Completion Guidance:*

*Selection of any of the In Place responses for Requirement 4.2.1 means the merchant has confirmed that strong cryptography and security controls are implemented to safeguard PAN during transmission over open, public networks **either** because 1) the controls are enabled and active on the PTS POI device or 2) the merchant has implemented controls that provide this functionality.*

# Maintain a Vulnerability Management Program

## Requirement 6: Develop and Maintain Secure Systems and Software

| PCI DSS Requirement | Expected Testing | Response[♦] *(Check one response for each requirement)* | | | |
|---|---|---|---|---|---|
| | | In Place | In Place with CCW | Not Applicable | Not in Place |
| **6.3** Security vulnerabilities are identified and addressed. | | | | | |
| *Note:* For SAQ B-IP, this requirement applies to the merchant's firewall/router devices that connect PTS POI devices to the payment processor. *Identification and management of security vulnerabilities for PTS POI devices are often handled by the merchant's terminal provider or processor. The merchant should contact the entity managing its terminals to understand how this requirement is met and the responsibilities of the merchant and of the entity managing the terminals.* | | | | | |
| **6.3.1** Security vulnerabilities are identified and managed as follows:<br><br>• New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).<br>• Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.<br>• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.<br>• *Bullet intentionally left blank for this SAQ.* | • Examine policies and procedures.<br>• Interview responsible personnel.<br>• Examine documentation.<br>• Observe processes. | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes**<br><br>This requirement is not achieved by, and is in addition to, performing vulnerability scans according to Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability. | | | | | |

---

[♦] *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 |
| **6.3.3** | All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:<br><br>• Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.<br><br>• *Bullet intentionally left blank for this SAQ.* | • Examine policies and procedures.<br>• Examine system components and related software.<br>• Compare list of security patches installed to recent vendor patch lists. | ☐ | ☐ | ☐ | ☐ |

# Implement Strong Access Control Measures

## Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

| PCI DSS Requirement | | Expected Testing | Response[♦] *(Check one response for each requirement)* | | | |
|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not in Place |
| **7.2** Access to system components and data is appropriately defined and assigned. | | | | | | |
| **7.2.2** | Access is assigned to users, including privileged users, based on: <br> • Job classification and function. <br> • Least privileges necessary to perform job responsibilities. | • Examine policies and procedures. <br> • Examine user access settings, including for privileged users. <br> • Interview responsible management personnel. <br> • Interview personnel responsible for assigning access. | ☐ | ☐ | ☐ | ☐ |

---

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

## Requirement 8: Identify Users and Authenticate Access to System Components

| PCI DSS Requirement | Expected Testing | Response♦ *(Check one response for each requirement)* | | | |
|---|---|---|---|---|---|
| | | In Place | In Place with CCW | Not Applicable | Not in Place |
| **8.1** Processes and mechanisms for identifying users and authenticating access to system components are defined and understood. | | | | | |
| **8.1.1** All security policies and operational procedures that are identified in Requirement 8 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | • Examine documentation.<br>• Interview personnel. | ☐ | ☐ | ☐ | ☐ |
| ***SAQ Completion Guidance:***<br>*Selection of any of the In Place responses for Requirement 8.1.1 means that the merchant has policies and procedures in place that govern merchant activities for Requirement 8.* | | | | | |

---

♦ *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 |
| **8.2** User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle. | | | | | |
| **8.2.2** Group, shared, or generic IDs, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:<br>• ID use is prevented unless needed for an exceptional circumstance.<br>• Use is limited to the time needed for the exceptional circumstance.<br>• Business justification for use is documented.<br>• Use is explicitly approved by management.<br>• Individual user identity is confirmed before access to an account is granted.<br>• Every action taken is attributable to an individual user. | • Examine user account lists on system components and applicable documentation.<br>• Examine authentication policies and procedures.<br>• Interview system administrators. | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes** | | | | | |
| This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. | | | | | |
| **8.2.7** Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows:<br>• Enabled only during the time period needed and disabled when not in use.<br>• Use is monitored for unexpected activity. | • Interview responsible personnel.<br>• Examine documentation for managing accounts.<br>• Examine evidence. | ☐ | ☐ | ☐ | ☐ |

| PCI DSS Requirement | | Expected Testing | Response♦ *(Check one response for each requirement)* | | | |
|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not in Place |
| **8.4** Multi-factor authentication (MFA) is implemented to secure access into the CDE. | | | | | | |
| **8.4.3** | MFA is implemented for all remote access originating from outside the entity's network that could access or impact the CDE. | • Examine network and/or system configurations for remote access servers and systems.<br>• Observe personnel (for example, users and administrators) and third parties connecting remotely to the network. | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes**<br><br>The requirement for MFA for remote access originating from outside the entity's network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE. This includes all remote access by personnel (users and administrators), and third parties (including, but not limited to, vendors, suppliers, service providers, and customers).<br><br>If remote access is to a part of the entity's network that is properly segmented from the CDE, such that remote users cannot access or impact the CDE, MFA for remote access to that part of the network is not required. However, MFA is required for any remote access to networks with access to the CDE and is recommended for all remote access to the entity's networks.<br><br>The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function. | | | | | |

## 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: <br>• Documented. <br>• Kept up to date. <br>• In use. <br>• Known to all affected parties. | • Examine documentation. <br>• 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._ | | | | | |
| **9.2** Physical access controls manage entry into facilities and systems containing cardholder data. | | | | | |
| **9.2.2** Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility. | • Interview responsible personnel. <br>• Observe locations of publicly accessible network jacks. | ☐ | ☐ | ☐ | ☐ |
| **9.4** Media with cardholder data is securely stored, accessed, distributed, and destroyed. | | | | | |
| _Note: For SAQ B-IP, 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. <br>• Examine logs or other documentation. <br>• 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 |
| **9.4.2** | All media with cardholder data is classified in accordance with the sensitivity of the data. | • Examine documented procedures.<br>• Examine media logs or other documentation. | ☐ | ☐ | ☐ | ☐ |
| **9.4.3** | Media with cardholder data sent outside the facility is secured as follows:<br>　• *Bullet intentionally left blank for this SAQ.*<br>　• Media is sent by secured courier or other delivery method that can be accurately tracked.<br>　• *Bullet intentionally left blank for this SAQ.* | • Examine documented procedures.<br>• Interview personnel.<br>• Examine records.<br>• Examine offsite tracking logs for all media. | ☐ | ☐ | ☐ | ☐ |
| **9.4.4** | Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals). | • Examine documented procedures.<br>• Examine offsite media tracking logs.<br>• Interview responsible personnel. | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes**<br><br>Individuals approving media movements should have the appropriate level of management authority to grant this approval. However, it is not specifically required that such individuals have "manager" as part of their title. | | | | | |

| | 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:<br>• Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.<br>• Materials are stored in secure storage containers prior to destruction. | • Examine the media destruction policy.<br>• Observe processes.<br>• Interview personnel.<br>• 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. | | | | | |
| **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:<br>• Maintaining a list of POI devices.<br>• Periodically inspecting POI devices to look for tampering or unauthorized substitution.<br>• Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices. | • Examine documented policies and procedures. | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes**<br><br>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<br><br>These requirements do not apply to:<br>• Components used only for manual PAN key entry.<br>• 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:<br>• Make and model of the device.<br>• Location of device.<br>• Device serial number or other methods of unique identification. | • Examine the list of POI devices.<br>• Observe POI devices and device locations.<br>• Interview personnel. | ☐ | ☐ | ☐ | ☐ |
| **9.5.1.2** POI device surfaces are periodically inspected to detect tampering and unauthorized substitution. | • Examine documented procedures.<br>• Interview responsible personnel.<br>• 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:<br><br>• Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.<br>• Procedures to ensure devices are not installed, replaced, or returned without verification.<br>• Being aware of suspicious behavior around devices.<br>• Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel. | • Review training materials for personnel in POI environments.<br>• Interview responsible personnel. | ☐ | ☐ | ☐ | ☐ |

**SAQ Completion Guidance:**

*Selection of any of the In Place responses for Requirements at 9.5 means that the merchant has policies and procedures in place for Requirements 9.5.1, 9.5.1.1, 9.5.1.2, and 9.5.1.3, and that they maintain a current list of devices, conduct periodic device inspections, and train employees about what to look for to detect tampered or substituted devices.*

# Regularly Monitor and Test Networks

## Requirement 11: Test Security of Systems and Networks Regularly

| PCI DSS Requirement | Expected Testing | Response[♦]<br>*(Check one response for each requirement)* | | | |
|---|---|---|---|---|---|
| | | In Place | In Place with CCW | Not Applicable | Not in Place |
| **11.3** External and internal vulnerabilities are regularly identified, prioritized, and addressed. | | | | | |
| **11.3.2** External vulnerability scans are performed as follows:<br>• At least once every three months.<br>• By a PCI SSC Approved Scanning Vendor (ASV).<br>• Vulnerabilities are resolved and *ASV Program Guide* requirements for a passing scan are met.<br>• Rescans are performed as needed to confirm that vulnerabilities are resolved per the *ASV Program Guide* requirements for a passing scan. | • Examine ASV scan reports. | ☐ | ☐ | ☐ | ☐ |
| **Applicability Notes**<br><br>For the initial PCI DSS assessment against this requirement, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s).<br><br>However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred.<br><br>ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer.<br><br>Refer to the *ASV Program Guide* published on the PCI SSC website for scan customer responsibilities, scan preparation, etc. | | | | | |

---

[♦] *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 |
| **11.4** External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected. | | | | | | |
| **11.4.5** | If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:<br>• At least once every 12 months and after any changes to segmentation controls/methods.<br>• Covering all segmentation controls/methods in use.<br>• *Bullet intentionally left blank for this SAQ.*<br>• Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.<br>• Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).<br>• Performed by a qualified internal resource or qualified external third party.<br>• Organizational independence of the tester exists (not required to be a QSA or ASV). | • Examine segmentation controls.<br>• Review penetration-testing methodology.<br>• Examine the results from the most recent penetration test.<br>• 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 account 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:<br>• Established.<br>• Published.<br>• Maintained.<br>• Disseminated to all relevant personnel, as well as to relevant vendors and business partners. | • Examine the information security policy.<br>• Interview personnel. | ☐ | ☐ | ☐ | ☐ |
| **12.1.2** The information security policy is:<br>• Reviewed at least once every 12 months.<br>• Updated as needed to reflect changes to business objectives or risks to the environment. | • Examine the information security policy.<br>• 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.<br>• Interview responsible personnel.<br>• 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.

| | PCI DSS Requirement | Expected Testing | In Place | In Place with CCW | Not Applicable | Not in Place |
|---|---|---|---|---|---|---|
| **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 business 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.

| | PCI DSS Requirement | Expected Testing | In Place | In Place with CCW | Not Applicable | Not in Place |
|---|---|---|---|---|---|---|
| **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.<br>• Examine list of TPSPs. | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes**<br><br>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:<br>• Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.<br>• 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.<br>• 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.<br><br>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.<br><br>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.<br>• Examine evidence.<br>• 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.<br>• Examine documentation.<br>• Interview responsible personnel. | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes**<br><br>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.<br>• Examine documentation.<br>• Interview responsible personnel. | ☐ | ☐ | ☐ | ☐ |

*SAQ Completion Guidance:*

*Selection of any of the In Place responses for requirements at 12.8.1 through 12.8.5 means that the merchant has a list of, and agreements with, service providers it shares 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.<br>• Interview personnel.<br>• 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

| PCI DSS Requirement | | Expected Testing | Response♦ *(Check one response for each requirement)* | | | |
|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not in Place |
| **A2.1** POI terminals using SSL and/or early TLS are not susceptible to known SSL/TLS exploits. | | | | | | |
| **A2.1.1** | Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols. | ▪ Examine documentation (for example, vendor documentation, system/network configuration details) that verifies the devices are not susceptible to any known exploits for SSL/early TLS. | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | | | | |
| | This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.1.2 and A2.1.3 apply to POS POI service providers and are intentionally not included in this SAQ. The allowance for POS POI terminals that are not currently susceptible to exploits is based on currently known risks. If new exploits are introduced to which POS POI terminals are susceptible, the POS POI terminals will need to be updated immediately. | | | | | |

---

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

## *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 B-IP merchant assessments.

# Section 3: Validation and Attestation Details

## Part 3. PCI DSS Validation

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

Based on the results documented in the SAQ B-IP 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:***

| | |
|---|---|
| ☐ | **Compliant:** 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 **COMPLIANT** rating; thereby *(Merchant Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ. |
| ☐ | **Non-Compliant:** 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 **NON-COMPLIANT** rating; thereby *(Merchant Company Name)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ. |

**Target Date** for Compliance: *YYYY-MM-DD*

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 *before completing Part 4.*

| | |
|---|---|
| ☐ | **Compliant but with Legal exception:** 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 **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Merchant Company Name)* 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. *If selected, complete the following:*

| Affected Requirement | Details of how legal constraint prevents requirement from being met |
|---|---|
| | |
| | |
| | |

## Part 3a. Merchant Acknowledgement

**Signatory(s) confirms:**

*(Select all that apply)*

| | |
|---|---|
| ☐ | *PCI DSS Self-Assessment Questionnaire B-IP, 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. <br> 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. <br> 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 | |
| 1 | Install and maintain network security controls | ☐ | ☐ | |
| 2 | Apply secure configurations to all system components | ☐ | ☐ | |
| 3 | Protect stored account data | ☐ | ☐ | |
| 4 | Protect cardholder data with strong cryptography during transmission over open, public networks | ☐ | ☐ | |
| 6 | Develop and maintain secure systems and software | ☐ | ☐ | |
| 7 | Restrict access to system components and cardholder data by business need to know | ☐ | ☐ | |
| 8 | Identify users and authenticate access to system components | ☐ | ☐ | |
| 9 | Restrict physical access to cardholder data | ☐ | ☐ | |
| 11 | Test security systems and networks regularly | ☐ | ☐ | |
| 12 | Support information security with organizational policies and programs | ☐ | ☐ | |
| Appendix A2 | Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections. | ☐ | ☐ | |

*\* 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/](https://www.pcisecuritystandards.org/about_us/).