Completing the Self-Assessment Questionnaire

Merchant Eligibility Criteria for Self-Assessment Questionnaire A

Self-Assessment Questionnaire (SAQ) A includes only those PCI DSS requirements applicable to merchants with account data functions completely outsourced to PCI DSS validated and compliant third parties, where the merchant retains only paper reports or receipts with account data.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present) and do not store, process, or transmit any account data in electronic format on their systems or premises.

This SAQ is not applicable to face-to-face channels.

This SAQ is not applicable to service providers.

SAQ A merchants confirm that, for this payment channel:

- The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of account data is entirely outsourced to PCI DSS compliant third-party service provider (TPSP)/payment processor;
- The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions;
- The merchant has reviewed the PCI DSS Attestation of Compliance form(s) for its TPSP(s) and confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant; and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of the payment page(s)/form(s) delivered to the customer's browser originate only and directly from a PCI DSS compliant TPSP/payment processor.

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.

Note: *For this SAQ, PCI DSS Requirements that address the protection of computer systems (for example, Requirements 2, 6, and 8) apply to e-commerce merchants that redirect customers from their website to a third party for payment processing, and specifically to the merchant web server upon which the redirection mechanism is located. Mail order/telephone order (MOTO) or e-commerce merchants that have completely outsourced all operations (where there is no redirection mechanism from the merchant to the third party) and therefore do not have any systems in scope for this SAQ, would consider these requirements to be "not applicable." Refer to guidance on the following pages for how to report requirements that are not applicable.*

For SAQ A and e-commerce channels, PCI DSS requirements that refer to the "cardholder data environment" are applicable to the merchant website(s) that provides the address (the URL) of the TPSP's payment page/form to merchant customers. This is because the merchant website impacts how the account data is transmitted, even though the website itself does not receive account data.

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 the cardholder data environment (CDE). 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 A.
   - 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.
In Place with Remediation	The requirement was Not in Place when the expected testing was initially performed, but the merchant addressed the situation and put processes in place to prevent re-occurrence prior to completion of the self-assessment. In all cases of In Place with Remediation, the merchant has identified and addressed the reason the control failed, has implemented the control, and has implemented ongoing processes to prevent re-occurrence of the control failure. All responses in this column require a supporting explanation in Appendix C of this SAQ.
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 D 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 D: 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 restriction is one where meeting the PCI DSS requirement would violate a local or regional law or regulation.*

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 Appendix 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*

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.