SmartSuite

Framework / Cybersecurity / PCI Security Standards

PCI DSS v4.0.1 Self-Assessment Questionnaire D for Merchants and Attestation of Compliance

SAQ D for Merchants is the full PCI DSS v4.0.1 self-assessment, covering all twelve requirements and Appendix A2, for merchants that do not meet the criteria of any shorter SAQ.



What it is

PCI DSS v4.0.1 Self-Assessment Questionnaire D for Merchants (SAQ D) is the questionnaire for merchants that are eligible to self-assess but do not meet the criteria for any other SAQ type; it reproduces all twelve requirements of PCI DSS v4.0.1 plus Appendix A2, and it is the merchant form closest to a full Report on Compliance. The PCI Security Standards Council (PCI SSC) published the October 2024 edition with the other v4.0.1 SAQs on October 15, 2024; since January 1, 2025 they are the only SAQs accepted, PCI DSS v4.0 having retired on December 31, 2024. It is a validation tool with an Attestation of Compliance (AOC), not a standard.

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Assessment / Maturity Model

VERSION
v4.0.1 SAQ D for Merchants (October 2024)

EFFECTIVE
January 1, 2025 (the only SAQs accepted after PCI DSS v4.0 retired on December 31, 2024)

DOMAIN
Cybersecurity

FAMILY
PCI Security Standards

REGION
Global

INDUSTRY
Payment & FinTech

ADOPTION MODEL
Industry Requirement

IMPLEMENTATION COMPLEXITY
High

Source: pcisecuritystandards.org/document_library/?category=saqs

Why it matters

- **Eligibility by exclusion** SAQ D applies to merchants eligible to complete an SAQ that do not meet the criteria for any other SAQ type; the four examples in the Merchant Eligibility Criteria include e-commerce sites that accept account data and merchants with electronic storage.
- **Every requirement in one form** Section 2 covers Requirements 1 to 12 in the Council's six goal groups, and Appendix A2 covers POS POI terminals using SSL or early TLS; Part 2g of the AOC summarizes the responses for each.
- **Not Applicable must be proven** A requirement is Not Applicable only after verification: to mark the wireless requirements 1.3.3, 2.3.1, 2.3.2 and 4.2.1.2 Not Applicable the merchant first confirms that no wireless technology is used in or connects to its cardholder data environment, and every such answer is explained in Appendix C.
- **Partial assessments are possible** Not Tested is available when a requirement was excluded without consideration, for example when the acquirer asks for validation of Prioritized Approach milestones only; each is explained in Appendix D and the assessment is declared Partial in Section 3.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports PCI DSS 4.0.1 SAQ D (Merchants)

Requirement Register (Requirements 1 to 12 and A2)

One record per Section 2 requirement with the response chosen, the Expected Testing performed, evidence attached and the Appendix C or D explanation where Not Applicable or Not Tested was selected.

Scope and Segmentation File (Parts 2c and 2d)

Describe the cardholder data environment, its connections, in-scope facilities and segmentation so the scoping confirmation in completion step 2 is documented.

Validated Products List (Part 2e)

Track each PCI SSC listed product or solution in use with its listing reference number and expiry date, and flag expiries before the next assessment.

Vulnerability and Scan Tracker

Use Cyber & IT Risk to hold ASV scan results, rescans and remediation on the quarterly cadence of Requirement 11.3.2, ready to submit with the SAQ.

TPSP Register (Part 2f and 12.8)

Use Third Party Risk Management for every provider that stores, processes or transmits account data or could affect its security, with agreements and annual compliance status.

Attestation Dashboard (Section 3 and Part 4)

Show the Full or Partial status, requirements still Not in Place, target dates for the Part 4 action plan and the annual submission deadline to the acquirer.

Common framework mappings

ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

PCI DSS v4.0.1 Documentation Library

Provides comprehensive PCI DSS v4.0.1 standards and supporting documents for compliance.

pcisecuritystandards.org/document_library

PCI DSS Requirements and Security Assessment Procedures

Defines the specific requirements and assessment procedures for PCI DSS v4.0.1 compliance.

pcisecuritystandards.org/document_library/?category=pcidss&document=pci_dss

PCI DSS Self-Assessment Questionnaires

Outlines self-assessment procedures for verifying PCI DSS compliance by entity type.

pcisecuritystandards.org/document_library?category=saqs

PCI Documentation Frequently Asked Questions

Provides answers to common questions regarding PCI DSS documentation and compliance.

pcisecuritystandards.org/faqs

Frequently asked questions

When must a merchant use SAQ D instead of a shorter SAQ?

When it is eligible to self-assess but does not meet the criteria for any other SAQ type. The Merchant Eligibility Criteria give four examples: e-commerce merchants that accept account data on their website, merchants with electronic storage of account data, merchants that do not store account data electronically but meet no other SAQ, and merchants that might meet another SAQ but have additional applicable PCI DSS requirements. The acquirer or payment brand confirms which SAQ, if any, a merchant may use.

What is the difference between Not Applicable and Not Tested in SAQ D?

Not Applicable means the requirement does not apply to the environment and this has been verified; for example, the wireless requirements 1.3.3, 2.3.1, 2.3.2 and 4.2.1.2 can be Not Applicable only after the merchant confirms no wireless technology is used in or connects to its cardholder data environment, and each answer is explained in Appendix C. Not Tested means the requirement was excluded from the assessment without considering whether it applies, as when an acquirer asks for only certain Prioritized Approach milestones; each is explained in Appendix D and the assessment becomes a Partial assessment, declared in Section 3.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Which appendices of SAQ D for Merchants apply to a merchant?

Appendix A2 applies to merchants whose POS POI terminals use SSL or early TLS: A2.1.1 asks the merchant to confirm the devices are not susceptible to known exploits, while A2.1.2 and A2.1.3 are for service providers only. Appendix A1 (multi-tenant service providers) is not used for merchant assessments, and Appendix A3 applies only to entities a payment brand or acquirer designates for supplemental validation. Appendix B is the Compensating Controls Worksheet, Appendix C explains Not Applicable responses and Appendix D explains Not Tested responses.

What goes into the Attestation of Compliance for SAQ D?

Section 1 holds Parts 1 and 2: contacts, the payment channels assessed and excluded, how account data is handled, the environment and segmentation, in-scope facilities, PCI SSC validated products in use, third-party service providers and the Part 2g summary of responses per requirement and for Appendix A2. Section 3 holds Parts 3 and 4: the Full or Partial declaration, the compliance status, the merchant's acknowledgement that SAQ D Version 4.0.1 was completed per its instructions, the executive officer's signature, any QSA or ISA involvement and, if requested after a Non-Compliant result, an action plan with remediation dates for Requirements 1 to 12.

Can a merchant use the customized approach or compensating controls in SAQ D?

Compensating controls, yes: a requirement met with a compensating control is reported as In Place with CCW and a Compensating Controls Worksheet is completed in Appendix B, following PCI DSS Appendices B and C. The customized approach, no: the SAQ states that SAQs cannot be used to document the customized approach and that its objectives are therefore not included; an entity wishing to use it may be able to use the Report on Compliance template, subject to the rules of its acquirer or the payment brands.

License included / downloadable: Yes SAQ D for Merchants is published by the PCI Security Standards Council and is downloadable free of charge from the Council's Document Library once its license agreement is accepted.

Full framework page and mappings: smartsuite.com/frameworks/pci-dss-v4-0-1-saq-d-merchants-cardholder-data-security-controls

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.