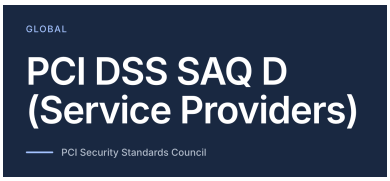
PCI DSS v4.0.1 Self-Assessment Questionnaire D for Service Providers and Attestation of Compliance

SAQ D for Service Providers is the only PCI DSS v4.0.1 SAQ a service provider may use: all twelve requirements, Appendix A1 for multi-tenant providers, Appendix A2 and described results.



What it is

PCI DSS v4.0.1 Self-Assessment Questionnaire D for Service Providers is the only SAQ a service provider may use: it applies to all service providers that a payment brand defines as eligible to complete a self-assessment, and it validates against every requirement of PCI DSS v4.0.1 , with Appendix A1 for multi-tenant service providers and Appendix A2 added. The current text is Revision 2 of January 2025; the first v4.0.1 edition came out with the other SAQs on October 15, 2024, and since January 1, 2025 the v4.0.1 SAQs are the only ones accepted, PCI DSS v4.0 having retired on December 31, 2024. The SAQ is a validation form 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 Service Providers, Revision 2 (January 2025)

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

- **One SAQ, no eligibility test** Any service provider that a payment brand deems eligible to self-assess uses this form; the question is not which SAQ but whether a Report on Compliance is required instead.
- **Scope declared per service** Part 2a lists the services included and excluded, by type (hosting, managed services, payment processing, payment gateway or switch and others), and Part 2g is completed once for each service assessed, with a Justification for Approach for every Not Applicable or Not Tested answer.
- **Environment evidence up front** Section 2a collects network diagrams, the storage-of-account-data table with encryption and access logging per data store, any sensitive authentication data storage, in-scope system component types with counts and vendors, and the quarterly ASV scans with Attestations of Scan Compliance.
- **Results described, not just ticked** The Service Provider Required Reporting column requires a brief description of how testing and evidence demonstrate each response, including which aspect a compensating control covered and why any requirement was excluded.

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

How SmartSuite supports PCI DSS 4.0.1 SAQ D (Service Providers)

Service Scope Register (Part 2a)

One record per service with its category, whether it is included in the assessment, the reason for any exclusion and its own Part 2g summary.

Environment Evidence (Section 2a)

Store the network diagrams, the account data storage table with encryption and logging per data store, system component types with counts and vendors, and the quarterly ASV scan records.

Requirement and Results Register (Section 2b)

One record per requirement with the response, the Describe Results text, evidence and the Appendix C or D explanation where needed, with the service-provider-only items flagged.

Multi-Tenant Controls (Appendix A1)

Track logical separation, per-customer access, the six-monthly separation penetration test, per-customer audit logs and the customer channel for reporting incidents and vulnerabilities.

Customer Acknowledgments (12.9.1 and 12.8.5)

Use Third Party Risk Management to hold the written agreements that acknowledge responsibility for customer account data and the record of which requirements the provider, the customer or both manage.

Attestation and Action Plan (Section 3 and Part 4)

Dashboard of Full or Partial status, requirements Not in Place, remediation dates by requirement and appendix, and the submission to the payment brand or acquirer.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | FedRAMP Rev. 5 | HIPAA | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | 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

Can a service provider use any SAQ other than SAQ D?

No. The Service Provider Eligibility Criteria state that SAQ D for Service Providers applies to all service providers defined by a payment brand as eligible to complete an SAQ and that it is the only SAQ option for service providers; the first completion step repeats this. The alternative is not a shorter SAQ but a Report on Compliance with a Qualified Security Assessor, and the payment brands and acquirers decide which route a provider must take.

What does Section 2a of SAQ D for Service Providers require?

Section 2a, Details about Reviewed Environment, asks for network diagrams showing all connections to the cardholder data environment and the security controls at each boundary; a table of every database, file or other data store holding account data, with the elements stored, how they are secured and how access is logged; whether sensitive authentication data is stored after authorization or for issuer functions; a list of in-scope system component types with counts, vendors and roles; and the quarterly ASV scans of the last twelve months with any failed scans and rescans, plus the Attestations of Scan Compliance. The April 2022 edition added this section for service provider self-assessments.

© 2026 SmartSuite Inc. All rights reserved.

Who must complete Appendix A1 and what does it ask?

Multi-tenant service providers, which PCI DSS describes as third-party service providers whose customers share system resources, infrastructure, applications or databases; providers offering only shared data center space are excluded. A1.1 requires logical separation between provider and customers (A1.1.1), per-customer access to its own cardholder data and environment (A1.1.2) and resources (A1.1.3), and penetration testing of the separation controls at least once every six months (A1.1.4); A1.2 requires audit log capability per customer (A1.2.1), support for forensic investigations (A1.2.2) and a secure channel for customers to report incidents and vulnerabilities, remediated per Requirement 6.3.1 (A1.2.3). A1.1.1 and A1.1.4 were best practice until March 31, 2025.

What changed in Revision 1 and Revision 2 of the v4.0.1 SAQ D for Service Providers?

Both are errata. Revision 1 (December 2024) corrected a requirement number reference in Requirement 3.6.1.1, a service-provider-only item. Revision 2 (January 2025) corrected the date recorded for that change in the Document Changes table and made the table of contents clickable. The requirement content is that of the October 2024 edition, which aligned the SAQ with PCI DSS v4.0.1 and added the ASV Resource Guide to its resource list.

What is the Describe Results column and why is it there?

Section 2b gives every requirement a Service Provider Required Reporting instruction: briefly describe how the testing and evidence demonstrate that the requirement is In Place or Not in Place, which aspect a compensating control covered, the testing that shows a requirement is Not Applicable, or why a requirement was excluded as Not Tested. The Document Changes table records that the column was added in April 2022 so that service providers describe their testing results; merchant SAQs do not have it.

License included / downloadable: Yes The PCI Security Standards Council publishes SAQ D for Service Providers in its Document Library; the PDF is free to download after the Council's license agreement is accepted.

Full framework page and mappings: smartsuite.com/frameworks/pci-dss-4-0-1-saq-d-service-providers

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