SmartSuite

Framework / Cybersecurity / PCI Security Standards

PCI DSS v4.0.1 Self-Assessment Questionnaire C and Attestation of Compliance

PCI DSS v4.0.1 SAQ C is the questionnaire and attestation for merchants with an Internet-connected payment application in a single store; it covers all twelve requirements in reduced form.



What it is

PCI DSS v4.0.1 Self-Assessment Questionnaire C (SAQ C) is the questionnaire and Attestation of Compliance for merchants whose payment application system, for example a point-of-sale (POS) system, is connected to the Internet, and who do not store account data electronically. The SAQ is a validation tool published by the PCI Security Standards Council rather than a standard: a merchant that meets its Merchant Eligibility Criteria uses it to self-assess against the applicable requirements of PCI DSS v4.0.1 and to attest the result to the payment brand or acquirer that manages its compliance program. It cannot be used for e-commerce channels or by service providers.

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Standard

VERSION
v4.0.1 SAQ C (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
Medium

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

Why it matters

- **Twelve requirements, one store** The criteria require that the physical POS location is not connected to other premises and that any LAN is for a single store only, so the full set of requirements is applied to a bounded environment.
- **Segmentation defines the edge** The payment application system must be isolated from all other merchant systems, which the criteria say can be achieved by network segmentation; Requirement 11.4.5 then requires that segmentation to be penetration-tested at least every 12 months.
- **Logging sized to the merchant** Requirement 10 is included, with log retention of at least 12 months and the most recent three months immediately available (10.5.1), but the central log server backup requirement 10.3.3 was removed in October 2024.
- **Risk analysis only where the standard asks for it** Requirement 12.3.1 requires a documented targeted risk analysis for each requirement that calls for one, reviewed at least once every 12 months, rather than a general enterprise risk assessment.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports PCI DSS 4.0.1 SAQ C

Eligibility and Store Scope (Parts 2c and 2h)

Document the single-store LAN, the device that hosts the payment application and Internet connection, the segmentation that isolates it, and the five criteria the merchant certifies.

Twelve-Requirement Response Set (Section 2 and Part 2g)

Keep each included sub-requirement as a record with its one response, Expected Testing evidence, Appendix B worksheet or Appendix C explanation, and roll the responses up into the Part 2g summary.

Configuration Standards and Change Records (2.2.1, 6.5.1, 6.5.2)

Hold the configuration standards for system components and a change log with reason, security impact, approval and post-change confirmation for the production environment.

Scans, Patches and Log Reviews (11.3.1, 11.3.2, 6.3.3, 10.4)

File the quarterly internal and ASV scan reports with rescans, critical patch dates, and the daily log review records and exception follow-ups.

Targeted Risk Analysis Records (12.3.1)

Record each analysis with the assets, threats, likelihood and impact factors and the justification for the frequency chosen, and schedule the review at least every 12 months.

Providers and Attestation (12.8, Parts 3 and 4)

Maintain the service provider list, agreements and compliance status, and capture the Part 3 status, signatures and any Part 4 remediation dates.

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 Self-Assessment Questionnaire (SAQ C)

Provides detailed security controls for merchant cardholder data within payment applications.

pcisecuritystandards.org/document_library

PCI DSS v4.0 Summary of Changes

Outlines the changes and updates from PCI DSS version 3.2.1 to 4.0.

pcisecuritystandards.org/document_library

PCI DSS Resources

Provides access to PCI DSS standards and supporting documents.

pcisecuritystandards.org/pci_security/standards_overview

PCI SSC FAQ

Answers frequently asked questions regarding PCI DSS implementation and compliance.

pcisecuritystandards.org/faqs

Frequently asked questions

Which merchants qualify for PCI DSS SAQ C?

Under the Merchant Eligibility Criteria, SAQ C is for merchants whose payment application system, such as a POS system, and Internet connection are on the same device and/or the same LAN, where that system is isolated from all other merchant systems, the POS location is not connected to other premises and any LAN serves a single store, no account data is stored electronically, and any retained account data is on paper. Both card-present and mail or telephone order merchants can use it; e-commerce channels and service providers cannot.

Why does SAQ C include all twelve requirements when SAQ B-IP has ten?

SAQ C's environment is a merchant-run payment application on a networked, Internet-connected device, so the anti-malware controls of Requirement 5 and the audit logging controls of Requirement 10 apply, alongside Requirements 1 to 4, 6 to 9, 11 and 12. SAQ B-IP covers standalone PTS-validated terminals, and the Council left Requirements 5 and 10 out of that form. Each SAQ states that it includes only the requirements that apply to its defined environment.

 © 2026 SmartSuite Inc. All rights reserved.

Which requirement was removed from SAQ C in the October 2024 edition?

The Document Changes table says the October 2024 edition deleted Requirement 10.3.3, which had been added when the SAQ was updated for PCI DSS v4.0, because it is not relevant for SAQ C merchants. In the standard, 10.3.3 requires audit log files to be promptly backed up to a secure, central, internal log server or other media that is difficult to modify. The Council's bulletin of 15 October 2024 describes this as the one requirement removed from any SAQ in the v4.0.1 set.

What scanning and testing does SAQ C require?

Requirement 11.2.1 and 11.2.2 require testing for and inventorying wireless access points. Requirement 11.3.1 requires internal vulnerability scans at least every three months with high-risk and critical findings resolved and rescanned, and 11.3.2 requires external scans at least every three months by a PCI SSC Approved Scanning Vendor. Requirement 11.4.5 requires a penetration test of segmentation controls at least every 12 months where segmentation is used, and 11.5.2 requires a change-detection mechanism on critical files.

What does the targeted risk analysis in Requirement 12.3.1 involve?

For each PCI DSS requirement that specifies a targeted risk analysis, 12.3.1 requires a documented analysis that identifies the assets being protected and the threats the requirement guards against, the factors that affect likelihood and impact, and the resulting justification for the frequency or process the merchant has chosen. Each analysis must be reviewed at least once every 12 months to confirm the results are still valid.

License included / downloadable: No SAQ C and its Attestation of Compliance are distributed by the PCI Security Standards Council through its Document Library, free of charge once the Council's license terms are accepted; the text is not supplied with the platform.

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