SmartSuite

Framework / Cybersecurity / PCI Security Standards

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

PCI DSS v4.0.1 SAQ B-IP is the questionnaire and attestation for merchants using only standalone, PCI-listed PTS terminals with an IP link to the processor; it covers ten requirements.



What it is

PCI DSS v4.0.1 Self-Assessment Questionnaire B-IP (SAQ B-IP) is the questionnaire and Attestation of Compliance for merchants whose only card acceptance runs through standalone, PCI-listed PIN Transaction Security (PTS) point-of-interaction (POI) devices that connect to the payment processor over IP, with no account data stored electronically. Like every SAQ it is a validation tool, not a standard: Section 2 reproduces the requirements of PCI DSS v4.0.1 that the PCI Security Standards Council considers applicable to this environment, and the merchant reports the outcome to the acquirer or payment brand that runs its compliance program. Merchants using devices classified as Secure Card Readers (SCR) or Secure Card Readers for PIN (SCRP) are excluded, as are e-commerce channels and service providers (Merchant Eligibility Criteria).

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Assessment / Maturity Model

VERSION
v4.0.1 SAQ B-IP (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
Low

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

Why it matters

- **Ten requirements, scoped to the terminal network** Requirements 1, 2, 3, 4, 6, 7, 8, 9, 11 and 12 appear, with far fewer sub-requirements than the full standard; for example Requirement 8 asks for 8.1.1, 8.2.2, 8.2.7 and 8.4.3 only.
- **PTS validation carries weight** The devices must be validated under the PTS POI program and appear on the PCI SSC list; footnote 1 tells merchants with expired approvals to check with their acquirer or payment brand whether this SAQ is still acceptable.
- **Segmentation is allowed, and then tested** The criteria allow the terminals to be isolated from other systems by network segmentation, and Requirement 11.4.5 then requires a penetration test of the segmentation controls at least every 12 months and after changes.
- **Future-dated items are handled in the form** Under Guidance for Responding to Future Dated Requirements, a bullet not yet implemented before 31 March 2025 could be marked Not Applicable and explained in Appendix C.

How SmartSuite supports PCI DSS 4.0.1 SAQ B-IP

PTS Device Register (Part 2h and 9.5.1.1)

Record each terminal with its PTS approval listing, expiry, location and serial number, so the eligibility certification and the device list draw on one source and expired approvals are visible.

Ten-Requirement Response Set (Section 2)

Keep the sub-requirements of Requirements 1 to 4, 6 to 9, 11 and 12 as records with one response each, the evidence named in Expected Testing, and the Appendix B worksheet or Appendix C explanation where used.

Network Diagram and Segmentation Tests (1.2.3, 11.4.5)

Store the current network diagram, the list of approved services, protocols and ports, and the results of the penetration tests of segmentation controls with their dates.

ASV Scans and Patch Records (11.3.2, 6.3.1, 6.3.3)

File each quarterly ASV scan report and rescan, the vulnerability risk rankings and the dates critical patches were applied to the devices and network components.

Service Providers and Third-Party Accounts (12.8, 8.2.7)

Maintain the provider list with agreements, compliance status and the requirements each provider manages, and log when third-party accounts were enabled, monitored and disabled.

Attestation Record (Parts 3 and 4)

Hold the compliance status, the executive officer's signature date, any QSA or ISA role, and the remediation dates for Not in Place items that a Part 4 action plan would list.

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 B-IP)

Provides guidance for assessing cardholder data security controls for standalone IP-connected terminals.

pcisecuritystandards.org/document_library

PCI Data Security Standard Requirements and Testing Procedures v4.0

Defines comprehensive security requirements for protecting cardholder data in payment environments.

pcisecuritystandards.org/document_library

PCI DSS Quick Reference Guide

Describes key concepts and security requirements of PCI DSS v4.0.

pcisecuritystandards.org/document_library?document=pci_dss_qrg

Frequently asked questions

Which merchants may use SAQ B-IP, and which devices are excluded?

The Merchant Eligibility Criteria admit merchants that take card payments only through standalone, PCI-listed approved PTS point-of-interaction devices connected to the processor over IP, where the devices are isolated from other systems, send account data only to the processor, do not rely on a computer, phone or tablet to connect, and no account data is stored electronically. Devices classified as Secure Card Readers (SCR) or Secure Card Readers for PIN (SCRP) are excluded, and so are e-commerce channels and service providers. A merchant with an expired PTS approval should ask its acquirer or payment brand whether this SAQ remains acceptable.

Which PCI DSS requirements are in SAQ B-IP, and which are left out?

Section 2 contains Requirements 1, 2, 3, 4, 6, 7, 8, 9, 11 and 12, each limited to the sub-requirements relevant to IP-connected terminals. Requirement 5 (anti-malware) and Requirement 10 (audit logging) are not included. Part 2g of the Attestation of Compliance summarizes the responses for the ten requirements.

 © 2026 SmartSuite Inc. All rights reserved.

Does SAQ B-IP require vulnerability scans?

Yes. Requirement 11.3.2 requires external vulnerability scans at least once every three months by a PCI SSC Approved Scanning Vendor, resolution of findings to the ASV Program Guide's passing standard, and rescans as needed. For the first assessment the applicability note accepts a single most recent passing scan if scanning policies exist and findings were corrected; in later years passing scans every three months must have occurred. If segmentation is used, Requirement 11.4.5 adds a penetration test of the segmentation controls at least every 12 months.

What changed in the October 2024 edition of SAQ B-IP?

The Document Changes table records that the October 2024 edition was updated to align with PCI DSS v4.0.1 and added the ASV Resource Guide to the Additional PCI SSC Resources section. Two earlier revisions of the v4.0 form also matter: December 2022 removed In Place with Remediation as a response and added guidance on future-dated requirements, and January 2024 restored Requirement 4.2.1, which had been left out of the v4.0 edition by mistake. SAQ B-IP was not among the questionnaires whose eligibility criteria the Council clarified in October 2024.

How does SAQ B-IP handle future-dated requirements?

Each future-dated bullet in Section 2 carries the note that it is a best practice until 31 March 2025, after which it is required. Before that date a merchant that had not implemented such an item could mark it Not Applicable and record the reason in Appendix C. In SAQ B-IP the example is the bullet in Requirement 4.2.1 requiring that certificates used to protect PAN over open, public networks are valid and not expired or revoked.

License included / downloadable: No SAQ B-IP and its Attestation of Compliance are available from the PCI SSC Document Library as a free download once the Council's license agreement is accepted; the document is not bundled with the platform.

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

© 2026 SmartSuite Inc. All rights reserved.