SmartSuite

Framework / Cybersecurity / PCI Security Standards

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

PCI DSS v4.0.1 SAQ B is the self-assessment questionnaire and attestation for merchants using only imprint machines or standalone dial-out terminals; it covers Requirements 3, 7, 9 and 12.



What it is

PCI DSS v4.0.1 Self-Assessment Questionnaire B (SAQ B) is the validation tool for merchants that take card payments only through imprint machines or standalone dial-out terminals connected to the processor over a phone line, keep no account data in electronic form, and report their compliance with PCI DSS v4.0.1 to an acquirer or payment brand by self-assessment. It is not a standard of its own: the PCI Security Standards Council's bulletin of 15 October 2024 calls the SAQs validation tools for SAQ-eligible merchants and service providers, and Section 2 of the questionnaire mirrors the requirements of PCI DSS. The Merchant Eligibility Criteria state that SAQ B does not apply to e-commerce channels or to service providers.

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Assessment / Maturity Model

VERSION
v4.0.1 SAQ B (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

- **Four requirements instead of twelve** Section 2 contains Requirements 3, 7, 9 and 12 of PCI DSS; network, cryptography, anti-malware, software, authentication, logging and testing requirements do not appear because the terminal is not connected to the merchant's systems or the Internet.
- **A paper-only data footprint** The criteria require that any account data the merchant retains is on paper, such as printed receipts or reports, and that nothing is received electronically; Requirement 3 therefore applies only to merchants that keep such paper records.
- **A written eligibility test** Part 2h of the AOC repeats the five criteria as a certification the merchant signs, so the choice of SAQ B is itself documented and reviewable.
- **One response per requirement** Each requirement takes exactly one response, and any Not Applicable answer needs an explanation in the appendix provided for it, which keeps the record complete for the acquirer.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports PCI DSS 4.0.1 SAQ B

Eligibility Record (Part 2h)

Keep the five SAQ B criteria as a checklist per payment channel, with the date confirmed and the evidence that the terminals are dial-out only and not connected to other systems or the Internet.

Requirement Responses (Section 2)

Hold the sub-requirements of Requirements 3, 7, 9 and 12 as records, each with its single response, its Expected Testing evidence and the explanation an appendix requires for Not Applicable or compensating control answers.

POI Device List and Inspections (9.5.1)

Track each terminal with make, model, location and serial number, log the periodic surface inspections of 9.5.1.2, and record the training given under 9.5.1.3.

Service Provider Register (12.8)

Maintain the list of third-party service providers from Part 2f, their written agreements, due diligence, PCI DSS compliance status and the requirements each one manages for the merchant.

Policies, Awareness and Incident Plan (12.1, 12.6, 12.10)

Store the information security policy with its review dates, the security awareness program records and the incident response plan so the Requirement 12 responses point to current documents.

Attestation and Action Plan (Parts 3 and 4)

Record the compliance status declared in Part 3, the signatories and dates, and any Not in Place requirement with its remediation date for the Part 4 action plan.

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 Standard

Defines the requirements for payment card security standards and related assessment procedures.

pcisecuritystandards.org/document_library

PCI DSS v4.0.1 Self-Assessment Questionnaire Instructions and Guidelines

Provides detailed guidance on completing the self-assessment questionnaire.

pcisecuritystandards.org/document_library

PCI DSS v4.0.1 Summary of Changes

Outlines the major updates and changes from previous versions.

pcisecuritystandards.org/document_library

Frequently asked questions

Which merchants are eligible to use PCI DSS SAQ B?

The Merchant Eligibility Criteria limit SAQ B to merchants that take payment card information only through an imprint machine and/or standalone dial-out terminals connected to the processor by a phone line, where the terminals are not connected to any other system in the merchant environment or to the Internet, no account data is stored electronically, and any retained account data is on paper and not received electronically. The merchant certifies these points in Part 2h of the Attestation of Compliance. SAQ B does not apply to e-commerce channels or to service providers.

Which PCI DSS requirements does SAQ B include?

Section 2 contains Requirement 3 (protect stored account data, applicable only to merchants with paper records), Requirement 7 (restrict access by business need to know), Requirement 9 (restrict physical access to cardholder data, including the media controls in 9.4.1 to 9.4.6 and the point-of-interaction device controls in 9.5.1) and Requirement 12 (policies, awareness, third-party service providers and incident response). Part 2g of the AOC summarizes the responses for those four requirements.

 © 2026 SmartSuite Inc. All rights reserved.

How does SAQ B differ from SAQ B-IP?

SAQ B is for terminals that dial out to the processor over a phone line, while SAQ B-IP is for standalone PTS-approved point-of-interaction devices with an IP connection to the processor. Because an IP connection puts the device on a network, SAQ B-IP adds Requirements 1, 2, 4, 6, 8 and 11, including external vulnerability scans by an Approved Scanning Vendor, which SAQ B does not contain.

What are the response options and when is a requirement Not Applicable?

The merchant selects one response for each requirement; the options defined in the Requirement Responses table include In Place, In Place with a Compensating Controls Worksheet (Appendix B), Not Applicable and Not in Place, and Not Tested is not available because every requirement in SAQ B must be tested. The SAQ's own example of Not Applicable is Requirements 9.4.1 to 9.4.6, which apply only when the merchant stores paper media with cardholder data; each Not Applicable response needs a written explanation in the appendix provided.

What happens after the questionnaire is completed?

Section 3 holds Parts 3 and 4 of the Attestation of Compliance. In Part 3 the merchant declares Compliant, Non-Compliant with a target date for compliance, or Compliant but with Legal exception, and an executive officer signs Part 3b; a QSA or ISA that assisted is recorded in Parts 3c and 3d. Part 4, the action plan for non-compliant requirements, is completed only when the organization receiving the AOC asks for it. The SAQ and AOC are then submitted to the payment brand or acquirer that manages the merchant's compliance program.

License included / downloadable: No The PCI Security Standards Council publishes SAQ B and its Attestation of Compliance in the PCI SSC Document Library, where it can be downloaded free of charge after accepting the Council's license agreement; the text is not included with the platform.

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