SmartSuite

Framework / Cybersecurity / PCI Security Standards

PCI DSS v4.0.1 – SAQ B-IP

PCI DSS SAQ B-IP specifies security controls for protecting cardholder data on standalone IP-connected payment terminals.

What it is

PCI DSS v4.0.1 Self-Assessment Questionnaire (SAQ B-IP) is a cybersecurity and compliance assessment tool that enables merchants with standalone IP-connected payment terminals to validate their handling of cardholder data and adherence to critical security controls. The SAQ B-IP specifically addresses the unique requirements for securing card data in environments with minimal payment processing systems connected via IP.

Developed and published by the PCI Security Standards Council, the PCI DSS SAQ B-IP is used by merchants, compliance teams, and assessors to evaluate technical and procedural safeguards related to data protection, network security, and compliance oversight. Its focus areas include securing payment terminals, managing network access, protecting stored cardholder data, and enabling compliance with the broader PCI DSS ecosystem.

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Assessment / Maturity Model

VERSION
v4.0.1

EFFECTIVE
June 11, 2024

DOMAIN
Cybersecurity

FAMILY
PCI Security Standards

REGION
The specific jurisdiction associated with the **PCI DSS v4.0.1 Self-Assessment Questionnaire (SAQ B-IP)**—namely, the issuing “region” of this regulation or framework—is: United States

INDUSTRY
Payment & FinTech

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: https://www.pcisecuritystandards.org/document_library

Why it matters

- **Strengthen cardholder data protection** Reduce the risk of unauthorized access and data exposure by implementing targeted controls for IP-connected payment terminal environments.
- **Simplify compliance scope** Focus PCI DSS assessment requirements on systems and processes specific to SAQ B-IP scope, reducing compliance complexity.
- **Enhance visibility and oversight** Establish clear accountability for monitoring and managing security controls protecting cardholder data in terminal environments.

How SmartSuite supports PCI DSS 4.0 SAQ B-IP

SAQ B-IP Control Library

Organize PCI DSS controls specific to standalone IP-connected terminal environments.

Payment Environment Scoping and Segmentation

Define cardholder data environment (CDE) boundaries and track network segmentation controls.

Terminal Security and Configuration Management

Track secure configurations, device hardening, and approved payment terminal controls.

Vulnerability and Patch Management for Payment Systems

Monitor vulnerabilities, patch status, and remediation activities for connected payment systems.

Evidence Collection and SAQ Documentation

Capture required evidence and responses supporting SAQ B-IP self-assessment submissions.

Compliance Reporting and Attestation Readiness

Provide dashboards showing control status, gaps, and readiness for PCI attestation.

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

What is PCI DSS v4.0.1 SAQ B-IP used for?

PCI DSS v4.0.1 SAQ B-IP is used by merchants that process cardholder data solely via standalone IP-connected payment terminals. Its primary purpose is to establish the security controls necessary to protect cardholder data during payment transactions and maintain PCI DSS compliance.

Is PCI DSS SAQ B-IP mandatory or certifiable?

PCI DSS compliance, including SAQ B-IP, is mandatory for all organizations that store, process, or transmit cardholder data. Merchants use SAQ B-IP to self-assess their compliance, but a formal certification may still require validation and submission to acquiring banks or card brands as prescribed.

Who is eligible to use SAQ B-IP?

SAQ B-IP is applicable to merchants who use only standalone, PIN Transaction Security (PTS)-approved payment terminals with IP connectivity, and that have no electronic storage of cardholder data. Merchants with more complex environments or additional payment channels must use other appropriate SAQs.

What are the key security controls required by PCI DSS SAQ B-IP?

Key controls required by SAQ B-IP include secure configuration and management of payment terminals, strong network segmentation, firewall protection, encrypted communications, strong passwords, and maintaining updated anti-malware solutions. Physical security measures and restricted access to terminals are also essential.

 · © 2026 SmartSuite Inc. All rights reserved.

How should an organization implement PCI DSS SAQ B-IP controls?

Implementation involves performing an environment review, ensuring only eligible devices are in use, segmenting payment systems from other networks, configuring firewalls, and establishing security policies and procedures. Ongoing employee training and regular system monitoring are critical for sustained compliance.

How does SAQ B-IP relate to other PCI DSS SAQs or validation types?

SAQ B-IP is one of several PCI DSS Self-Assessment Questionnaires, each tailored for different merchant environments. Organizations should review all SAQ eligibility criteria to select the correct form; using the wrong SAQ may result in non-compliance.

What ongoing activities are required to maintain PCI DSS SAQ B-IP compliance?

Maintaining compliance requires annual completion of the SAQ, regular network and control monitoring, periodic vulnerability scans, staff security awareness training, and prompt remediation of identified issues. Documentation and evidence of ongoing compliance activities must be retained for review.

How would SmartSuite support PCI DSS v4.0.1 SAQ B-IP?

SmartSuite can help organizations manage PCI DSS SAQ B-IP requirements by tracking risks, assigning and monitoring control ownership, collecting compliance evidence, and maintaining audit trails. The platform supports audit readiness with centralized documentation, workflow automation, and compliance reporting to streamline assessment and validation processes.

License included / downloadable: Yes The PCI DSS v4.0.1 SAQ B-IP is published by the PCI Security Standards Council and is freely available for download from the PCI SSC website. License included with platform

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

© 2026 SmartSuite Inc. All rights reserved.