SmartSuite

Framework / Cybersecurity / PCI Security Standards

# PCI DSS v4.0.1 – SAQ B

PCI DSS SAQ B defines security controls for merchants using imprint machines and standalone dial-out terminals to protect cardholder data.

## What it is

PCI DSS v4.0.1 Self-Assessment Questionnaire (SAQ B) is a compliance assessment tool that supports organizations in evaluating cardholder data security controls specifically for imprint and standalone dial-out payment terminals. The questionnaire is part of the Payment Card Industry Data Security Standard, which establishes requirements for safeguarding payment card data and minimizing risks related to payment card processing environments.

Published by the PCI Security Standards Council, PCI DSS SAQ B is intended for merchants who do not store electronic cardholder data and only process card payments through non-integrated imprint or standalone dial-out terminals. The SAQ covers key areas such as physical security, device protection, and secure handling of cardholder information, ensuring that organizations meet industry-mandated cybersecurity and data protection obligations.

## At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Assessment / Maturity Model

VERSION
v4.0.1

EFFECTIVE
January 1, 2025

DOMAIN
Cybersecurity

FAMILY
PCI Security Standards

REGION
Payment Card Industry Data Security Standard (PCI DSS), including its Self-Assessment Questionnaire (SAQ) B—used for imprint machines and standalone dial-out terminals—is developed and managed by the PCI Security Standards Council (PCI SSC). The PCI SSC is an international, industry-driven body founded by major payment card brands (Visa, MasterCard, American Express, Discover, and JCB). It operates on a global basis and is not tied to any specific country or governmental jurisdiction ([en.wikipedia.org](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard?utm_source=openai)). Therefore, the Region Detail for PCI DSS v4.0.1 SAQ B reflects its nature as a globally applicable standard. The appropriate jurisdiction to record in the Region Detail field is: Global

INDUSTRY
Payment & FinTech

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

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

## Why it matters

- **Enhance cardholder data protection** Reduce the risk of unauthorized access and data exposure by implementing targeted

## How SmartSuite supports PCI DSS 4.0.1 SAQ B

### SAQ B Requirement Library

Structure PCI DSS SAQ B requirements with mapped controls, ownership, and compliance activities.

### Payment Terminal Asset Management

Maintain inventory of payment terminals and associated systems within the cardholder data environment.

### Physical and Device Security Governance

Track physical security controls protecting payment terminals from tampering or unauthorized access.

### Terminal Configuration and Security Monitoring

Manage terminal configuration standards, maintenance procedures, and device security monitoring.

### Vendor and Service Provider Oversight

Track payment processor and service provider compliance documentation and responsibilities.

### Self-Assessment and Compliance Reporting

Provide dashboards showing SAQ B completion status, requirement coverage, and outstanding compliance tasks.

## 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

### What is PCI DSS SAQ B used for?

PCI DSS SAQ B is designed for merchants who process cardholder data exclusively via imprint machines or standalone dial-out terminals with no electronic cardholder data storage. It helps organizations demonstrate compliance with the Payment Card Industry Data Security Standard (PCI DSS) requirements tailored to these environments, ensuring cardholder data is protected during processing.

### Is completing PCI DSS SAQ B mandatory?

Yes, completion of PCI DSS SAQ B is typically required for eligible merchants by payment brands and acquiring banks. Compliance is not optional and is a prerequisite for accepting payment cards in the specified manner.

### What environments are in scope for PCI DSS SAQ B?

SAQ B applies only to merchants that process card transactions using either manual imprint machines or standalone, dial-out payment terminals that connect directly to a payment processor and do not store cardholder data electronically. It excludes any environments with integrated point-of-sale systems, network connectivity, or electronic storage of cardholder data.

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

Key controls include restricting physical access to cardholder data, maintaining policies for device security, protecting devices from tampering, and ensuring that cardholder data is not stored electronically. Additionally, merchants must establish processes for incident response and periodically inspect devices.

 © 2026 SmartSuite Inc. All rights reserved. 

### How is PCI DSS SAQ B implemented in a merchant environment?

Implementation involves identifying all devices and processes in scope, applying the controls outlined in the SAQ, ensuring staff are trained on device security, and documenting procedures. Merchants should also regularly review compliance, inspect devices for tampering, and ensure no cardholder data is stored electronically.

### How does PCI DSS SAQ B relate to other PCI DSS SAQs?

SAQ B is one of several assessment questionnaires, each designed for a specific merchant environment. SAQ B is the most restrictive, with the narrowest scope, while other SAQs apply to merchants with more complex or integrated payment processing environments. Choosing the correct SAQ is critical for accurate attestation.

### What ongoing compliance activities are required for PCI DSS SAQ B?

Ongoing activities include periodic inspections of payment terminals, maintaining updated device lists, staff training, regular reviews of physical and procedural controls, and annual SAQ completion and attestation. Merchants must also promptly address any identified security risks or device tampering incidents.

### How would SmartSuite support PCI DSS SAQ B?

SmartSuite can support PCI DSS SAQ B compliance by providing tools for risk tracking, managing required controls, and tracking device inventories. It enables evidence collection for compliance activities, helps maintain audit readiness by documenting inspections and training, and streamlines reporting for annual attestation and ongoing monitoring.

License included / downloadable: Yes The PCI DSS SAQ B (v4.0.1) is published by the PCI Security Standards Council and is publicly available for free download from the Council's website. License included with platform

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