

PCI DSS v4.0 – SAQ A

PCI DSS SAQ A is a self-assessment for e-commerce merchants to validate outsourced cardholder data security controls.



What it is

PCI DSS v4.0 Self-Assessment Questionnaire (SAQ A) is a compliance assessment tool that helps eligible e-commerce merchants demonstrate adherence to the Payment Card Industry Data Security Standard by documenting the security controls protecting cardholder data. This questionnaire simplifies the PCI DSS compliance process for merchants who outsource all payment processing and have minimal contact with cardholder data.

Published by the PCI Security Standards Council, SAQ A is used by e-commerce merchants, acquiring banks, and compliance teams to verify that merchants meet the specific security requirements for handling card-not-present transactions. The assessment focuses on cybersecurity controls such as access control, data protection, and policies ensuring that cardholder data is neither stored nor processed within the merchant’s own IT environment.

At a glance

PUBLISHER Payment Card Industry Security Standards Council (PCI SSC)	TYPE Assessment / Maturity Model	VERSION v4.0
EFFECTIVE March 31, 2024	DOMAIN Cybersecurity	FAMILY PCI Security Standards
REGION Global	INDUSTRY Payment & FinTech	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

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

Why it matters

- Strengthen data protection practices** Reduce exposure to cardholder data by ensuring sensitive information is never stored, processed, or transmitted on merchant systems.
- Improve cybersecurity oversight** Provide merchants and stakeholders with clear visibility into the effectiveness of security controls across outsourced payment channels.
- Enhance audit readiness** Supply streamlined documentation and self-assessment evidence, simplifying regulatory reviews and supporting timely compliance reporting.
- Support third-party risk management** Enable organizations to assess and confirm the security posture of payment service providers handling cardholder transactions.

How SmartSuite supports PCI DSS 4.0 SAQ A

SAQ A Requirement Library

Organize PCI DSS v4.0 SAQ A requirements with mapped controls, owners, and implementation activities.

Payment Page Scoping and Architecture

Document payment page integrations, hosted payment providers, and cardholder data flow boundaries.

Vendor and Payment Processor Oversight

Track third-party payment service providers, compliance attestations, and contract obligations.

Security Control Evidence Collection

Capture policies, configuration documentation, and compliance artifacts supporting SAQ A requirements.

Payment Compliance Activity Tracking

Track identified risks, remediation tasks, and ongoing compliance activities affecting payment environments.

SAQ Readiness and Compliance Reporting

Provide dashboards summarizing SAQ readiness, requirement coverage, and outstanding compliance actions.

Common framework mappings

CIS Controls v8.1

COBIT 2019

FedRAMP Rev. 5

HIPAA (NIST SP 800-66 Rev. 2)

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-53 Rev.5

SOC 2

Official resources

PCI DSS v4.0 Requirements and Security Assessment Procedures

Official document outlining security requirements for protecting cardholder data.

pcisecuritystandards.org/document_library

PCI DSS Self-Assessment Questionnaire (SAQ) Instructions and Guidelines

Provides guidance for merchants completing the PCI DSS SAQ for compliance.

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 SAQ A used for?

PCI DSS v4.0 SAQ A is a self-assessment tool designed for e-commerce merchants who outsource all cardholder data functions to third-party service providers. It helps these merchants validate that no cardholder data is electronically stored, processed, or transmitted on their systems, while still maintaining responsibility for implementing specific security controls.

Is PCI DSS SAQ A mandatory for e-commerce merchants?

PCI DSS SAQ A is not a legal requirement but is mandated by major payment card brands as a part of their compliance programs. E-commerce merchants who meet the eligibility criteria must complete SAQ A to demonstrate compliance with PCI DSS requirements to acquiring banks or payment processors.

What types of organizations are eligible to use PCI DSS SAQ A?

Only e-commerce merchants that fully outsource their cardholder data handling to PCI DSS compliant third-party service providers and do not electronically store, process, or transmit cardholder data on their own systems are eligible for SAQ A. Merchants conducting in-person or mail/telephone order transactions are not eligible for this SAQ.

What security controls does PCI DSS SAQ A require?

SAQ A focuses on controls related to secure payment page redirection, maintaining information security policies, ensuring physical access controls, and ongoing security awareness training. The requirements are limited compared to other SAQs but still include critical measures such as ensuring that only trusted service providers are used and cardholder data is never stored locally.

How should an organization implement PCI DSS SAQ A requirements?

Implementation involves confirming that all cardholder data functions are outsourced and that no cardholder data touches the merchant environment. Merchants must verify service provider PCI DSS compliance, document their processes, train staff in security awareness, and maintain policies that enforce these requirements.

How does PCI DSS SAQ A relate to other PCI SAQs?

PCI DSS SAQ A represents the minimum set of controls for merchants with the simplest risk profile—those fully outsourcing cardholder data functions. Other SAQs, such as SAQ B or SAQ D, apply to merchants with more complex processing environments or greater involvement in handling cardholder data.

What are the ongoing requirements to remain compliant with PCI DSS SAQ A?

Ongoing compliance requires annual completion and submission of the SAQ, annual security training for relevant staff, maintaining up-to-date policies, and continuous monitoring to ensure no changes bring cardholder data processing into the merchant's own systems. Merchants must also stay current with PCI DSS updates and verify the continued compliance of their service providers.

How would SmartSuite support PCI DSS v4.0 SAQ A?

SmartSuite can help organizations manage PCI DSS SAQ A by providing centralized risk tracking, streamlined control implementation, and structured evidence collection for SAQ requirements. The platform's audit readiness features facilitate ongoing compliance monitoring, and reporting dashboards offer clear visibility into the organization's status for internal and external assessments.

License included / downloadable: Yes PCI DSS v4.0 SAQ A is publicly available for free from the PCI SSC website. License included with platform

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