SmartSuite

Framework / Cybersecurity / PCI Security Standards

PCI DSS v4.0.1 – SAQ C

SAQ C is a PCI DSS self-assessment questionnaire for assessing cardholder data security controls in payment application systems.

What it is

PCI DSS v4.0.1 Self-Assessment Questionnaire (SAQ C) is a compliance assessment tool that helps organizations validate the implementation of security controls for payment application systems that store, process, or transmit cardholder data. It is a key part of the Payment Card Industry Data Security Standard (PCI DSS), which aims to protect payment card information and reduce the risks of data breaches.

Published by the PCI Security Standards Council (PCI SSC), this questionnaire is intended for merchants with payment application systems connected to the internet but without electronic storage of cardholder data. SAQ C covers essential cybersecurity requirements, including data protection, access controls, network security, and regular monitoring, ensuring compliance with industry regulations for cardholder data environments.

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Standard

VERSION
v4.0.1

EFFECTIVE
June 11, 2024

DOMAIN
Cybersecurity

FAMILY
PCI Security Standards

REGION
PCI DSS v4.0.1 (including the Self-Assessment Questionnaire SAQ C) is issued and administered by the PCI Security Standards Council. This organization is headquartered in the United States. Therefore, the jurisdiction for this document is: United States

INDUSTRY
Payment & FinTech

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

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

Why it matters

- **Strengthen data protection practices** Safeguard cardholder data through robust controls, reducing the risk of unauthorized access or data breaches in payment environments.
- **Improve compliance support** Demonstrate adherence to PCI DSS requirements, enabling smoother assessments and reducing risk of non-compliance penalties.
- **Enhance incident response preparedness** Establish structured processes for timely detection and response to security

How SmartSuite supports PCI DSS 4.0.1 SAQ C

SAQ C Requirement Library

Structure SAQ C requirements with mapped controls, implementation tasks, and accountable owners.

Payment Application Scope Documentation

Document payment application systems, infrastructure components, and network boundaries supporting transactions.

Network Security and Monitoring Controls

Track firewall rules, segmentation controls, and monitoring protecting payment application systems.

Payment System Vulnerability and Patch Management

Manage vulnerability scanning, patch deployment, and remediation activities affecting payment systems.

Access Reviews and Authentication Management

Track user access reviews, authentication policies, and privileged access management.

PCI DSS SAQ C Compliance Reporting

Provide dashboards showing requirement coverage, remediation progress, and readiness for PCI DSS SAQ C assessments.

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 C)

Provides detailed security controls for merchant cardholder data within payment applications.

pcisecuritystandards.org/document_library

PCI DSS v4.0 Summary of Changes

Outlines the changes and updates from PCI DSS version 3.2.1 to 4.0.

pcisecuritystandards.org/document_library

PCI DSS Resources

Provides access to PCI DSS standards and supporting documents.

pcisecuritystandards.org/pci_security/standards_overview

PCI SSC FAQ

Answers frequently asked questions regarding PCI DSS implementation and compliance.

pcisecuritystandards.org/faqs

Frequently asked questions

What is PCI DSS v4.0.1 SAQ C used for?

PCI DSS v4.0.1 SAQ C is a self-assessment questionnaire designed for merchants with payment application systems that process cardholder data but do not store electronic cardholder data. It helps organizations validate their compliance with PCI DSS requirements specifically related to securing cardholder data during processing and transmission.

Is PCI DSS v4.0.1 SAQ C mandatory for all merchants?

PCI DSS v4.0.1 SAQ C is required for merchants that meet certain eligibility criteria, such as those whose payment application systems are connected to the internet and do not store cardholder data electronically. The use of this SAQ is determined by your acquirer or payment brand, so eligibility must be confirmed with them.

Who is eligible to use the PCI DSS v4.0.1 SAQ C?

SAQ C is applicable to merchants with payment application systems that are internet-connected, do not store electronic cardholder data, and process payments via standalone terminals or systems. Organizations that store cardholder data electronically, or use systems integrated with other network components, may need to use a different SAQ.

What types of controls are required under PCI DSS v4.0.1 SAQ C?

The SAQ C requires controls such as installing and maintaining secure systems, protecting cardholder data during transmission, maintaining vulnerability management programs, implementing strong access controls, monitoring security of systems, and maintaining an information security policy.

 Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How should merchants implement PCI DSS v4.0.1 SAQ C requirements?

Merchants should ensure that all payment application systems are securely configured, regularly patched, and segmented from other systems. Strong authentication, encryption for cardholder data in transit, and regular monitoring for unauthorized access or vulnerabilities are essential for effective compliance.

How does PCI DSS v4.0.1 SAQ C relate to other PCI DSS SAQs?

SAQ C is tailored for a specific merchant environment where payment applications are used and cardholder data is not stored electronically. Other SAQs, like SAQ A or SAQ B, apply to different setups, such as fully outsourced payment processing or standalone terminal environments. Selecting the correct SAQ is critical for accurate assessment.

What are the ongoing compliance requirements for PCI DSS v4.0.1 SAQ C?

Ongoing compliance involves conducting annual self-assessments, maintaining required security controls, performing quarterly network scans, and keeping documentation and evidence of compliance. Regular staff training and incident response procedures are also necessary to protect cardholder data consistently.

How would SmartSuite support PCI DSS v4.0.1 SAQ C?

SmartSuite can help organizations manage PCI DSS v4.0.1 SAQ C by enabling risk tracking, assigning and monitoring control implementation, and centralizing evidence collection for each control. It also supports audit readiness through structured workflows and provides real-time reporting to demonstrate ongoing compliance and streamline assessments.

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

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

 © 2026 SmartSuite Inc. All rights reserved.