

PCI DSS v4.0.1

PCI DSS v4.0.1 defines security requirements organizations must follow to protect payment card data during storage, processing, and transmission.



What it is

PCI DSS v4.0.1 is an international cybersecurity and data protection standard that enables organizations to secure payment card data and maintain effective controls for handling cardholder information. Its primary purpose is to reduce payment card fraud by establishing comprehensive requirements for protecting account data during storage, processing, and transmission.

Developed and maintained by the Payment Card Industry Security Standards Council (PCI SSC), PCI DSS is mandatory for merchants, service providers, and any entity that stores, processes, or transmits cardholder data. The standard addresses critical areas such as access control, cybersecurity monitoring, vulnerability management, encryption, and compliance oversight within payment environments.

At a glance

<div>PUBLISHER</div> <div>Payment Card Industry Security Standards Council (PCI SSC)</div>	<div>TYPE</div> <div>Standard</div>	<div>VERSION</div> <div>PCI DSS v4.0.1</div>
<div>EFFECTIVE</div> <div>2024</div>	<div>DOMAIN</div> <div>Cybersecurity</div>	<div>FAMILY</div> <div>PCI Security Standards</div>
<div>REGION</div> <div>Global</div>	<div>INDUSTRY</div> <div>Payment & FinTech</div>	<div>ADOPTION MODEL</div> <div>Regulatory Compliance</div>
<div>IMPLEMENTATION COMPLEXITY</div> <div>High</div>		

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

Why it matters

- Strengthen data protection practices** Enforce consistent controls to safeguard cardholder data throughout its lifecycle, lowering the risk of unauthorized exposure or loss.
- Improve security oversight** Provide a clear framework for monitoring security activities, access, and compliance efforts within payment processing environments.
- Increase audit readiness** Facilitate evidence gathering and reporting, streamlining the audit process and supporting sustained regulatory compliance efforts.
- Enhance incident detection and response** Establish continuous monitoring and response processes to identify, contain, and recover from potential payment-related security incidents promptly.

How SmartSuite supports PCI DSS 4.0.1

PCI Scope and Asset Inventory

Define the cardholder data environment and connected systems with clear boundaries.

Requirement Library and Ownership

Track PCI requirements with owners, procedures, and implementation evidence.

Testing and Validation Cadence

Schedule scans, pen tests, access reviews, and control checks with proof of completion.

Evidence Repository and Audit Trail

Centralize policies, configs, test results, and logs tied to each PCI requirement.

Exceptions and Compensating Controls

Document compensating controls, approvals, and remediation timelines.

Audit-Ready Reporting

Generate status views for QSAs, leadership, and internal stakeholders.

Common framework mappings

[CIS Controls v8.1](#)[ISO 27001:2022](#)[ISO 27002:2022](#)[ISO 27701](#)[MITRE ATT&CK](#)[NIST CSF 2.0](#)[NIST 800-53 Rev.5](#)[SOC 2](#)

Official resources

PCI DSS v4.0.1 Standard Document

Defines security requirements for safeguarding payment card data in IT systems.

pcisecuritystandards.org/document_library

PCI DSS v4.0.1 Summary of Changes from v3.2.1

Outlines key updates and modifications made in the transition to PCI DSS v4.0.1.

pcisecuritystandards.org/document_library

PCI DSS v4.0.1 Implementation Guide

Provides practical guidance for organizations implementing PCI DSS v4.0.1 standards.

pcisecuritystandards.org/document_library

PCI DSS v4.0.1 Self-Assessment Questionnaires

Offers a toolset for entities to assess compliance with PCI DSS v4.0.1 requirements.

pcisecuritystandards.org/document_library

Frequently asked questions

What is PCI DSS v4.0.1 used for?

PCI DSS v4.0.1 is used to protect payment card data by establishing uniform security requirements for organizations that store, process, or transmit cardholder information. Its primary aim is to reduce payment card fraud and data breaches through comprehensive controls covering the entire payment environment.

Is PCI DSS v4.0.1 mandatory for organizations handling payment card data?

Yes, PCI DSS v4.0.1 is mandatory for all merchants, service providers, and entities that handle payment card data. Compliance is required by payment card brands and acquiring banks as a contractual obligation.

Which organizations must comply with PCI DSS v4.0.1, and what is its scope?

Any entity that stores, processes, or transmits cardholder data must comply with PCI DSS v4.0.1. The scope includes all system components, people, and processes that interact with or impact the security of payment cardholder data.

What are the main control requirements of PCI DSS v4.0.1?

PCI DSS v4.0.1 is structured around 12 high-level requirements, which cover areas such as network security, access control, vulnerability management, encryption, and ongoing monitoring. Organizations must implement both technical and operational controls to address these requirements.

How does an organization implement PCI DSS v4.0.1?

Implementation involves identifying systems and processes in scope, mapping controls to PCI DSS requirements, conducting risk assessments, and establishing documented policies and procedures. Regular training, access management, and incident response planning are also vital elements of implementation.

How does PCI DSS v4.0.1 relate to other regulatory and security frameworks?

PCI DSS v4.0.1 often aligns with other standards, such as ISO 27001, NIST, and various data protection regulations. However, it is specifically focused on payment card data, and its controls are tailored to address unique payment environment risks.

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

Organizations must conduct annual risk assessments, complete periodic self-assessments or third-party audits, maintain evidence of control effectiveness, and remediate identified vulnerabilities. Continuous monitoring and prompt documentation updates are required to sustain compliance.

How would SmartSuite support PCI DSS v4.0.1?

SmartSuite facilitates PCI DSS v4.0.1 compliance by enabling organizations to map controls, track relevant risks, and collect evidence for audits. With reporting dashboards and compliance workflows, SmartSuite supports audit readiness and ongoing oversight, making it easier to manage findings, demonstrate compliance, and sustain required documentation.

License included / downloadable: Yes PCI DSS documentation is publicly available through official PCI SSC resources.

Full framework page and mappings: smartsuite.com/frameworks/pci-dss-v4-0-1-payment-card-industry-data-security-standard