

PCI DSS v3.2

PCI DSS v3.2 defines security requirements to protect payment cardholder data and secure payment environments.



What it is

PCI DSS v3.2 is an information security standard that helps organizations protect payment card data and reduce the risk of data breaches and fraud. Its primary purpose is to establish a baseline for secure handling and processing of credit, debit, and other payment card information.

Published by the PCI Security Standards Council (PCI SSC), PCI DSS applies to all entities that store, process, or transmit cardholder data, including merchants, service providers, and financial institutions. The standard outlines requirements covering security controls, network protections, access control measures, vulnerability management, and ongoing monitoring to support robust cybersecurity and compliance oversight.

At a glance

PUBLISHER Payment Card Industry Security Standards Council (PCI SSC)	TYPE Standard	VERSION v3.2
EFFECTIVE October 31, 2016	DOMAIN Cybersecurity	FAMILY PCI Security Standards
REGION Payment Card Industry (PCI) Data Security Standard (PCI DSS) v3.2 is issued and governed by the Payment Card Industry Security Standards Council (PCI SSC). The PCI SSC is headquartered in the United States, specifically in Wakefield, Massachusetts.([en.wikipedia.org](https://en.wikipedia.org/wiki/Payment_Card_Industry_Security_Standards_Council?utm_source=openai)) Therefore, the appropriate Region Detail for PCI DSS v3.2 is: United States	INDUSTRY Payment & FinTech	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High Source: https://www.pcisecuritystandards.org/document_library		

Why it matters

- **Strengthen payment security governance** Implement structured oversight and accountability for payment security controls across all systems handling cardholder data.
- **Enhance regulatory compliance** Support adherence to payment industry requirements, reducing the risk of penalties and demonstrating due diligence in data protection.
- **Improve threat detection capabilities** Implement monitoring controls and logging practices to identify and respond to unauthorized activity within payment environments.

How SmartSuite supports PCI DSS 3.2

CSF Control and Function Mapping

Organize controls and activities across the five NIST CSF functions and framework categories.

Risk Register and Asset Context

Link assets, business processes, and threats to CSF categories to prioritize risk management.

Security Program Workflows

Track implementation tasks across protection, monitoring, incident response, and recovery activities.

Continuous Monitoring and Detection

Capture monitoring outputs, alerts, and investigation records supporting the Detect function.

Incident Response and Recovery Coordination

Manage response playbooks, communications, and recovery actions across security teams.

Executive Cybersecurity Reporting

Provide dashboards showing CSF maturity, risk exposure, and improvement initiatives.

Common framework mappings

CIS Controls v8.1

COBIT 2019

FedRAMP Rev. 5

HIPAA

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-53 Rev.5

SOC 2

Official resources

PCI DSS v3.2 Standard Document

Defines the security requirements for cardholder data environments.
pcisecuritystandards.org/document_library

PCI DSS v3.2 Self-Assessment Questionnaire

Provides tools to evaluate PCI DSS compliance within an organization.
pcisecuritystandards.org/document_library

PCI DSS v3.2 Compliance Guide

Outlines steps for achieving compliance with PCI DSS v3.2 requirements.
pcisecuritystandards.org/document_library

Frequently asked questions

What is PCI DSS v3.2 used for?

PCI DSS v3.2 is a security standard designed to protect payment card data and ensure secure handling, processing, and storage of cardholder information. It is used by organizations that accept, process, store, or transmit credit card data to mitigate risks of data breaches and fraud.

Is PCI DSS v3.2 compliance mandatory?

PCI DSS v3.2 compliance is mandatory for all entities that store, process, or transmit cardholder data, as required by payment card brands and acquiring banks. Non-compliance can result in penalties, increased transaction fees, or the loss of the ability to process payment cards.

Who must comply with PCI DSS v3.2 and what is the scope?

Any organization that handles payment card information, including merchants and service providers, must comply with PCI DSS v3.2. The scope includes all systems, people, and processes that store, process, or transmit cardholder data, as well as any connected systems that might impact security.

What are the key requirements and controls of PCI DSS v3.2?

PCI DSS v3.2 outlines 12 main requirements covering areas such as building secure networks, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control, and regularly monitoring networks. Organizations must establish and document controls such as firewalls, encryption, and security policies.

How should organizations implement PCI DSS v3.2 controls?

Organizations should begin with a scoping exercise to identify systems and processes that fall under PCI DSS, followed by a gap analysis to determine required changes. Implementation involves putting technical, physical, and procedural controls in place, documented by policies and ongoing training for relevant staff.

How does PCI DSS v3.2 relate to other information security frameworks?

PCI DSS v3.2 often overlaps with other frameworks such as ISO 27001 and NIST in areas like access control, network security, and risk management. However, PCI DSS is industry-specific and focuses on payment card security, providing more prescriptive, detailed requirements for the cardholder data environment.

What is required to maintain ongoing PCI DSS v3.2 compliance?

Maintaining PCI DSS v3.2 compliance requires regular security assessments, periodic vulnerability scans, continuous monitoring, accurate documentation, and annual reports on compliance. Organizations should also manage changes, respond to security incidents, and update training to align with evolving threats and requirements.

How would SmartSuite support PCI DSS v3.2?

SmartSuite can support PCI DSS v3.2 management by enabling organizations to track risks, document and monitor security controls, collect evidence for each requirement, and maintain audit readiness. Its integrated reporting and workflow capabilities simplify compliance status updates and facilitate streamlined management of remediation activities.

License included / downloadable: Yes The PCI DSS v3.2 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-v3-2-payment-card-industry-data-security-standard