SmartSuite

Framework / Cybersecurity / PCI Security Standards

Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0.1

PCI DSS v4.0.1 (June 2024) is the current Payment Card Industry Data Security Standard: twelve requirements, two validation approaches and the dates that retired v4.0.



What it is

PCI DSS v4.0.1 is the current version of the Payment Card Industry Data Security Standard, the baseline of technical and operational requirements for protecting payment account data. It applies to every entity that stores, processes or transmits cardholder data or sensitive authentication data, or that could affect the security of that data (Section 2). The entities in scope include merchants, processors, acquirers, issuers and other service providers. The PCI Security Standards Council (PCI SSC) published it in June 2024 as a limited revision of v4.0; the Council's Summary of Changes records corrections, clarifications and updated guidance and states that no change in this version was categorized as an evolving requirement. v4.0 was retired on December 31, 2024, so assessments from January 1, 2025 are against v4.0.1 (Section 14, Table 6).

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Standard

VERSION
v4.0.1 (June 2024)

EFFECTIVE
January 1, 2025 (v4.0 retired December 31, 2024; future-dated requirements effective March 31, 2025)

DOMAIN
Cybersecurity

FAMILY
PCI Security Standards

REGION
Global

INDUSTRY
Payment & FinTech

ADOPTION MODEL
Industry Requirement

IMPLEMENTATION COMPLEXITY
High

Source: pcisecuritystandards.org/standards/pci-dss/

Why it matters

- **One current version** Section 14 states that v4.0.1 is the current version of the standard and that questions about the use of previous versions go to the organizations that manage compliance programs, such as payment brands and acquirers.
- **Two ways to meet a requirement** Section 8 sets out the defined approach, which follows the stated requirements and testing procedures, and the customized approach, which meets each requirement's Customized Approach Objective in the entity's own way and is intended for risk-mature entities.

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports PCI DSS 4.0.1

Requirement Library and Approach

Load the twelve principal requirements and their numbered sub-requirements with the applicability notes, mark each as defined or customized approach (Section 8), and assign an owner and status.

Scope and CDE Inventory

Record the system components, people and processes in the cardholder data environment (Section 4), the account data flows, and the annual scope confirmation required by Requirement 12.5.2.

Targeted Risk Analysis Records

Document each targeted risk analysis with the assets, threats, likelihood and impact factors and the justified frequency (Requirement 12.3.1), with a 12-month review date and a link to the requirement it governs.

Compensating Controls and Customized Controls

Keep the Appendix C worksheet for each compensating control and the Appendix D controls matrix and Requirement 12.3.2 analysis for each customized control, with the testing evidence the assessor reviews.

Timeframe Calendar

Schedule the activities Table 4 defines, such as internal vulnerability scans at least once every three months (Requirement 11.3.1) and the 12-month reviews of cipher suites and technologies (Requirements 12.3.3 and 12.3.4), with proof of completion.

Third-Party Service Provider Register

Maintain the list of TPSPs and the services each provides (Requirement 12.8.1), the written agreements and the Attestations of Compliance they share (Section 9), and the split of responsibilities between TPSP and customer that Section 4 expects to be documented.

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 changed between PCI DSS v4.0 and v4.0.1?

v4.0.1 is a limited revision. The Council's Summary of Changes (Revision 1, August 2024) records no change categorized as an evolving requirement; the changes are clarifications, guidance updates and formatting, such as correcting typographical errors, pointing to the Appendix G glossary instead of repeating definitions, changing 'SAD is not retained' to 'SAD is not stored' in Requirement 3.3.1, adding a Customized Approach Objective to 3.5.1.1 and moving the note on account data received through an unintended channel into Section 4.

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

When did PCI DSS v4.0.1 become the only version, and what happened on March 31, 2025?

Table 6 of the standard lists v4.0 as retired on December 31, 2024, so from January 1, 2025 assessments are against v4.0.1; the Council's October 15, 2024 bulletin confirms the v4.0 SAQs stayed active only until that retirement. Separately, a number of requirements carry the applicability note that they were a best practice until March 31, 2025, after which they are required and must be fully considered during an assessment, for example Requirement 12.3.1 on targeted risk analysis.

What is the difference between the defined approach and the customized approach?

Section 8 describes both. In the defined approach the entity implements controls to meet the requirement as stated and the assessor follows the defined testing procedures; compensating controls are available where a documented constraint prevents meeting a requirement (Appendix B). In the customized approach the entity meets the requirement's Customized Approach Objective in its own way, maintains a controls matrix and a targeted risk analysis under Requirement 12.3.2 (Appendix D), and the assessor derives the testing procedures. Some requirements have no Customized Approach Objective and can only be met the defined way.

What is a targeted risk analysis under Requirement 12.3.1?

It is the documented analysis an entity performs for each PCI DSS requirement that lets the entity decide how often an activity is performed. Requirement 12.3.1 requires it to identify the assets being protected, the threats the requirement protects against, the factors that contribute to likelihood or impact, and the justification for the chosen frequency, and to review each analysis at least once every 12 months. The guidance distinguishes it from a traditional enterprise-wide risk assessment.

Who decides whether an organization must comply with or validate to PCI DSS v4.0.1?

Section 2 states that whether any entity is required to comply with or validate compliance is at the discretion of the organizations that manage compliance programs, such as payment brands and acquirers. The entity then follows the Section 12 process: confirm scope, assess, complete a Report on Compliance or a Self-Assessment Questionnaire, complete the Attestation of Compliance and submit it to the requesting organization. The standard also notes that where its requirements conflict with country, state or local law, the law applies (Section 1).

License included / downloadable: Yes PCI SSC publishes PCI DSS v4.0.1 free of charge; the PDF is downloaded from the PCI SSC Document Library after accepting the Council's license agreement.

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