SmartSuite

Framework / Cybersecurity / PCI Security Standards

Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures, Version 3.2 (superseded)

PCI DSS v3.2 (April 2016) is a retired version of the payment card data security standard, superseded by v3.2.1 in May 2018 and retired on January 1, 2019; the current version is v4.0.1.



What it is

PCI DSS v3.2 is a superseded version of the Payment Card Industry Data Security Standard: the current version is PCI DSS v4.0.1 , published in June 2024. The PCI Security Standards Council (PCI SSC) published v3.2 in April 2016 as an update from v3.1, and the Council's version table records that it was retired on December 31, 2018 (Table 6 of v4.0.1). The Council's December 2018 notice states that v3.2 remained valid through December 31, 2018, that entities could validate to either v3.2 or v3.2.1 before January 1, 2019, and that from that date all validations had to be to v3.2.1.

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Standard

VERSION
v3.2 (April 2016; superseded by v3.2.1 in May 2018 and retired January 1, 2019)

EFFECTIVE
Retired January 1, 2019

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

- **Multi-factor authentication for administrators** Requirement 8.3.1 required MFA for all non-console administrative access, mandatory from February 1, 2018 in every organization's assessment.
- **Change control that re-checks PCI DSS** Requirement 6.4.6 required change management processes to confirm that affected PCI DSS requirements are in place after a significant change.
- **Service provider accountability** Requirements 3.5.1, 10.8 and 10.8.1, 11.3.4.1, 12.4.1, 12.11 and 12.11.1 added cryptographic architecture documentation, control-failure detection, six-monthly segmentation testing, a formal compliance program and quarterly reviews for service providers.
- **An end to SSL and early TLS** After June 30, 2018 SSL and early TLS could not be used as a security control, except by POS POI terminals verified as not susceptible to known exploits and the termination points they connect to, as Appendix A2 defined.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports PCI DSS 3.2

Version Register

Record which PCI DSS version each past assessment, Report on Compliance and Attestation of Compliance was validated against, with the April 2016 to December 31, 2018 window for v3.2.

Requirement Crosswalk to v4.0.1

Map each v3.2 requirement number a report cites, such as 8.3.1 or 11.3.4.1, to the v4.0.1 requirement that now covers the control, so evidence moves without gaps.

Historical Evidence Archive

Keep v3.2-era policies, scan reports, compensating controls worksheets and attestations with their dates, separate from live evidence.

Service Provider Program Record

Carry forward the formal PCI DSS compliance program, quarterly reviews and control-failure detection that v3.2 introduced for service providers (12.4.1, 12.11, 10.8).

Protocol and Cryptography Inventory

Retain the SSL and early TLS migration record (Appendix A2, June 30, 2018) as the starting point for the cipher suite and protocol inventory v4.0.1 requires.

Migration Tracking to v4.0.1

Track the gaps closed between the v3.2 control set and v4.0.1, including the requirements that became mandatory after March 31, 2025.

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

Is PCI DSS v3.2 still valid?

No. The Council's version table (Table 6 of PCI DSS v4.0.1) lists v3.2 as retired on December 31, 2018, and its December 2018 notice states that from January 1, 2019 all validations had to be to v3.2.1. v3.2.1 and v4.0 have since retired as well, and PCI DSS v4.0.1 is the current version.

When was PCI DSS v3.2 published and when was it retired?

The Document Changes table of the current standard dates v3.2 to April 2016, as an update from v3.1. It remained valid through December 31, 2018 and was retired as of January 1, 2019, six months after v3.2.1 was published in May 2018.

What new requirements did PCI DSS v3.2 introduce, and when did they take effect?

They became mandatory on February 1, 2018. For all organizations: change management confirming that affected PCI DSS requirements are in place after significant change (6.4.6) and multi-factor authentication for all non-console administrative access (8.3.1). For service providers: a documented cryptographic architecture (3.5.1), detection and response to failures of critical security control systems (10.8, 10.8.1), segmentation penetration testing at least every six months (11.3.4.1), a formal PCI DSS compliance program (12.4.1) and at least quarterly reviews that security policies and procedures are followed (12.11, 12.11.1).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How did PCI DSS v3.2.1 differ from v3.2?

The Council described v3.2.1, published in May 2018, as a minor revision with no new requirements, made to account for dates that had already passed: the February 1, 2018 effective date for the new v3.2 requirements and the June 30, 2018 SSL and early TLS migration deadline. Entities could validate to either version until December 31, 2018; v3.2.1 then stood alone until it was retired on March 31, 2024.

Which version of PCI DSS should an organization assess against now?

PCI DSS v4.0.1. Section 14 of that standard names it the current version, v4.0 retired on December 31, 2024, and the requirements that were a best practice until March 31, 2025 are now required. The Section 14 note adds that questions about the use of previous versions should go to the organizations that manage compliance programs, such as payment brands and acquirers.

License included / downloadable: Yes PCI SSC publishes PCI DSS free of charge; the current documents are downloaded from the PCI SSC Document Library after accepting the Council's license agreement. v3.2 is retired, and the text to use is PCI DSS v4.0.1.

Full framework page and mappings: smartsuite.com/frameworks/pci-dss-v3-2-payment-card-industry-data-security-standard

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.