Get ready for PCI DSS v4.0.

What is the PCI Data Security Standard?

The Payment Card Industry Data Security Standard (PCI DSS) is a global standard that provides a baseline of technical and operational requirements designed to protect payment data. PCI DSS v4.0 is the next evolution of the Standard.

Goals for PCI DSS v4.0

- Promote security as a continuous process.
- Add flexibility for different methodologies.
- Enhance validation methods.
- Continue to meet the security needs of the payment industry.

Developed with global industry collaboration

Development of PCI DSS v4.0 was driven by industry feedback. This version furthers the protection of payment data with new controls to address sophisticated cyberattacks.

3
rounds of requests for comment on the draft content

6,000+
items of feedback received

200+
companies provided feedback

What is new in PCI DSS v4.0?

Many changes were incorporated into the latest version of the standard. Below are examples of some of those changes and why they were made.

Promote security as a continuous process.

Why it is important: Criminals never sleep. Ongoing security is crucial to protect payment data.

Example of changes in v4.0:

- Added guidance to help people better understand how to implement and maintain security

Increase flexibility for organizations using different methods to achieve security objectives.

Why it is important: This allows more customized options to achieve a requirement's objective and supports payment technology innovation.

Example of changes in v4.0:

- Customized approach, a new method to implement and validate PCI DSS requirements, provides flexibility for organizations using innovative methods to achieve security objectives

Enhance validation methods and procedures.

Why it is important: Clear validation and reporting options support transparency and granularity.

Example of changes in v4.0:

- Increased alignment between information reported in a Report on Compliance or Self-Assessment Questionnaire and information summarized in an Attestation of Compliance

Meet the changing security needs of the payments industry.

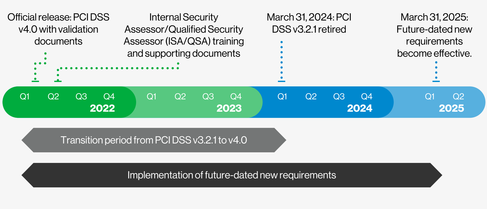
Why it is important: Security practices must evolve as threats change.

Example of changes in v4.0:

- New e-commerce and phishing requirements to address ongoing threats

Implementation timeline

PCI DSS v4.0 will go into effect two years after the March 31, 2022, publication date. Now is the time for organizations to become familiar with the new version and to begin planning for and implementing the changes needed.



Why Verizon

Verizon has one of the largest and most experienced PCI QSA teams in the world and has conducted more than 19,000 security assessments for companies of all sizes, including many Fortune 500 and multinational organizations.

We keep up with the rapidly changing nature of cyberthreats with the help of our analysis of more than 1 million security events every day at our global network operations centers and security operations centers. For over a decade, we've offered thought leadership on the issue with publications such as the Verizon Data Breach Investigations Report.

Learn more:

For more information on the Verizon PCI DSS Assessment, contact your Verizon Business Account Manager or visit:
verizon.com/business/products/security/cyber-risk-management/governance-risk-compliance/payment-card-industry-advisory-service/

Source: PCI Security Standards Council, 2022

verizon