PCI DSS v4.0

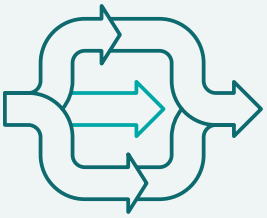
What is the PCI Data Security Standard?

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

Goals for PCI DSS v4.0

Continue to Meet the Security Needs of the Payment Industry

Promote Security as Continuous Process



Add Flexibility for Different Methodologies

Enhance Validation Methods

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 cyber attacks.

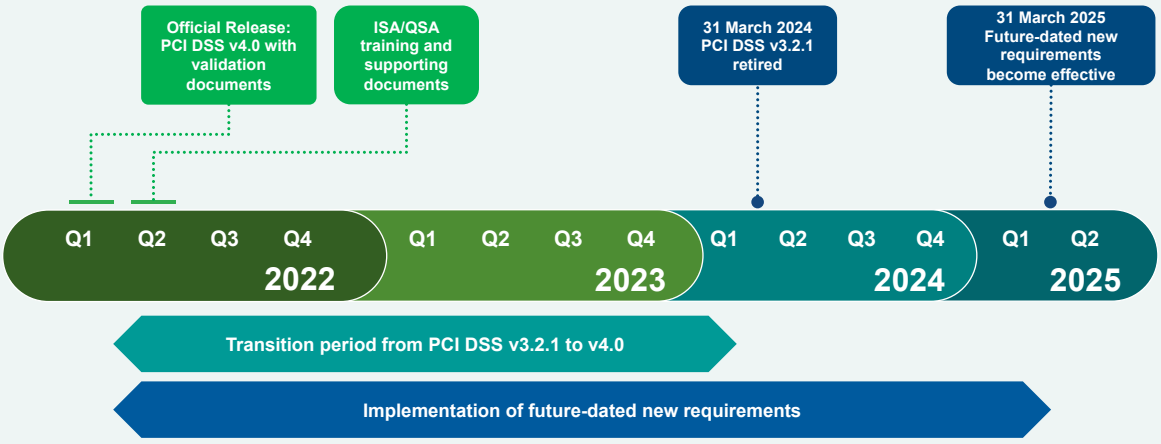
3
Request for Comment (RFCs) On Draft Content

6,000+
Items of Feedback Received

200+
Companies Provided Feedback

Implementation Timeline

PCI DSS v3.2.1 will remain active for two years after v4.0 is published. This provides organizations time to become familiar with the new version, and plan for and implement the changes needed.



What is New in PCI DSS v4.0?

There were many changes incorporated into the latest version of the Standard. Below are examples of some of those changes. For a comprehensive view, please refer to the Summary of Changes from PCI DSS v3.2.1 to v4.0, found in the **PCI SSC Document Library**.

Continue to meet the security needs of the payments industry.

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

Examples:

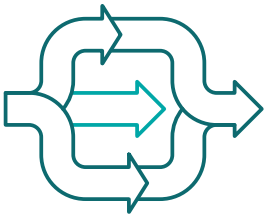
- Expanded multi-factor authentication requirements.
- Updated password requirements.
- New e-commerce and phishing requirements to address ongoing threats.

Promote security as a continuous process.

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

Examples:

- Clearly assigned roles and responsibilities for each requirement.
- Added guidance to help people better understand how to implement and maintain security.
- New reporting option to highlight areas for improvement and provide more transparency for report reviewers.



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

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

Examples:

- Allowance of group, shared, and generic accounts.
- Targeted risk analyses empower organizations to establish frequencies for performing certain activities.
- Customized approach, a new method to implement and validate PCI DSS requirements, provides another option 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:

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

Subscribe to the **PCI Perspectives Blog**