RSI | Datasheet

PCI DSS

Version 4

In March 2022, the Security Standards Council (SSC) of the Payment Card Industry (PCI) released its long-awaited update to the Data Security Standard (DSS). PCI DSS Version 4.0 builds upon the foundation of previous editions (most recently, 2018's v3.2.1), further strengthening security controls to protect cardholder data (CHD) and sensitive authentication data (SAD) across the cardholder data environment (CDE).

What's New in PCI DSS v4.0?

Ther SSC had four primary goals for DSS v4.0:

- Evolving to meet industry needs
- Ensuring ongoing CHD security
- Making implementation more flexible
- Enhancing compliance validation

To meet them, DSS v4.0 expanded several Requirements and Sub-Requirements and increased the range of compensating controls.

These priorities reflect over 6000 pieces of feedback from over 200 companies over the 3-year period comprising 3 Request for Comment (RFC) rounds.

When Will DSS v4.0 Be Required?

The projected timeline for DSS v4.0 rollout is:

Q1 2022 – DSS v4.0 and validation documents officially published (training documents pending)

Q1 2024 – DSS v3.2.1 officially retired; all ongoing assessments to require DSS v4.0

Q1 2025 – All future-dated new requirements for v4.0 are in full effect and assessed to full extent

In the transition period between Q1 2022 and Q1 2024, organizations seeking compliance will need to map existing controls from v3.2.1 onto any new Requirements or Sub-Requirements for v4.0.

How to Comply with PCI DSS 4.0

PCI DSS v4.0 Implementation

Defined Approach – The organization will implement all parts of the 12 Requirements, with appropriate compensating controls as needed.

Customized Approach – The organization will design and implement controls to meet the intended purpose of each Requirement.

In the latter case, the Qualified Security Assessor (QSA) defines appropriate procedures for testing whether customized controls meet DSS aims.

When Will DSS v4.0 Be Required?

There are two primary kinds of assessments an organization can conduct to verify compliance:

Self-Assessment Questionnaire (SAQ) – Merchants with the lowest transaction value may be eligible for self-assessment.

Report on Compliance (ROC) – Merchants and Service providers with higher annual transaction totals need to be assessed by a QSA.

In either case, the organization must submit an Attestation of Compliance (AOC) alongside the completed SAQ or ROC form.

Breakdown of PCI DSS 4.0 Requirements

Building Secure Networks

Requirement 1: Install network security controls

1.1: Define processes for maintaining security
1.2: Configure network security controls

Protecting Account Data

Requirement 3: Protect account data in storage

3.1: Define processes for protecting account data
3.2: Minimize account data kept in storage

1.3: Restrict network access
1.4: Control network connections
1.5: Mitigate risks from untrusted networks

Requirement 2: Use secure configurations

2.1: Define processes for secure configurations
2.2: Secure all system components
2.3: Secure wireless networks

Managing Vulnerabilities

Requirement 5: Protect against malicious software

5.1: Define processes for preventing malware
5.2: Prevent or detect and address all malware
5.3: Maintain active anti-malware processes
5.4: Utilize anti-phishing practices

Requirement 6: Maintain the security of systems

6.1: Define processes for secure development
6.2: Develop custom software securely
6.3: Identify and address vulnerabilities
6.4: Protect public-facing apps from attacks
6.5: Manage changes to system components

Monitoring Networks

Requirement 10: Monitor access to systems

10.1: Define processes for monitoring access
10.2: Implement audit logs for access monitoring
10.3: Protect audit logs from unauthorized access
10.4: Review audit logs for unauthorized activity
10.5: Ensure availability of audit log history
10.6: Implement accurate time synchronization
10.7: Detect, and respond to security failures

Requirement 11: Assess network security regularly

11.1: Define processes for security assessment
11.2: Identify and monitor wireless access points
11.3: Prioritize and address all vulnerabilities
11.4: Conduct penetration testing regularly
11.5: Detect and respond to file changes
11.6: Monitor for payment page changes

3.3: Do not store SAD after authorization
3.4: Restrict access to and ability to copy CHD
3.5: Secure Primary Account Numbers (PAN)
3.6: Use cryptographic keys for stored data
3.7: Implement cryptographic key management

Requirement 4: Encrypt data for transmission

4.1: Define processes for encrypting data
4.2: Use strong encryption to transmit PAN

Controlling User Access

Requirement 7: Restrict access by business need

7.1: Define processes for access restriction
7.2: Define and assign access appropriately
7.3: Manage access through a control system

Requirement 8: Authenticate users to grant access

8.1: Define processes for authenticating users
8.2: Manage access across account lifecycles
8.3: Utilize strong authentication measures
8.4: Require Multi-Factor Authentication (MFA)
8.5: Configure MFA systems to prevent misuse
8.6: Control authentication factors across apps

Requirement 9: Restrict physical access to systems

9.1: Define processes for physical restriction
9.2: Manage entry into CDE-related facilities
9.3: Manage physical access for staff and visitors
9.4: Store media containing CHD securely
9.5: Protect Point of Interaction (POI) devices

Managing Security Policy

Requirement 12: Support security with clear policies

12.1: Define processes for security policies
12.2: Define acceptable end-user use policies
12.3: Identify and manage risks to the CDE
12.4: Manage PCI DSS compliance actively
12.5: Document and scope PCI DSS compliance
12.6: Implement ongoing security education
12.7: Screen personnel for insider threats
12.8: Manage third-party service provider risks
12.9: Ensure third parties comply with PCI DSS
12.10: Respond to security incidents immediately

About RSI Security

RSI Security has assisted organizations in achieving PCI DSS compliance for over a decade. Our team of experts is recognized as a QSA and an Approved Scanning Vendor (ASV) by the PCI SSC, and we will help your organization with every step of the compliance process. We'll help you rethink your cybersecurity program for initial implementation, mapping from earlier DSS versions, or maintaining seamless compliance long-term.

www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com