PCI DSS 4.0.1
Compliance with RedSeal

PCI DSS 4.0.1 Overview

Version 4.0.1 of the Payment Card Industry Data Security Standard (PCI DSS) builds on the major changes introduced in version 4.0, while providing clarifications, corrections, and refinements to ensure consistent interpretation.
Organizations are now expected to:

- Define and document the scope of their cardholder data environment (CDE) using a formal **scoping methodology** (Req. 12.5.2).
- Retest segmentation controls whenever changes occur and verify that segmentation is effective in isolating the CDE (Req. 11.4.5).
- Perform **targeted risk analyses** to establish and document the frequency of specific security activities (Req. 12.3.1, 12.3.2).
- Enforce **multi-factor authentication** for all access into the CDE (Req. 8.4.2).
- Treat compliance as an ongoing, continuous process, supported by monitoring, metrics, and evidence gathering.

RedSeal enables organizations to meet these evolving requirements with efficiency and clarity.

Continuous Compliance ("Business-as-Usual")

Many organizations once treated PCI compliance as an annual project, preparing controls only in the weeks before an audit. PCI DSS 4.0.1 formalizes the expectation that compliance must be **continuous** and embedded into daily operations.

The standard's "business as usual" guidance requires:

- Monitoring security controls to ensure they function as intended.
- Detecting and remediating control failures promptly.
- Maintaining up-to-date network diagrams and inventories.
- Incorporating PCI DSS processes into change management and operational workflows.

RedSeal automates these practices, giving teams the evidence and visibility needed for year-round assurance.

Scope and Segmentation

Earlier versions of PCI DSS left segmentation guidance vague, leading to insecure implementations. Starting in v3.0, and strengthened in v4.0.1, the standard requires a **documented and rigorous segmentation strategy**:

- Segmentation must effectively isolate the CDE from out-of-scope systems.
- Organizations must follow a repeatable **scoping methodology** (Req. 12.5.2).
- Segmentation must be **validated after any change** and tested regularly (Req. 11.4.5).

RedSeal continuously validates segmentation across complex hybrid environments, ensuring scoping decisions remain accurate and defensible.

Highlights

PCI DSS 4.0.1 emphasizes continuous security, enhanced segmentation, and rigorous testing requirements. To help meet these challenges, RedSeal:

- Provides comprehensive PCI DSS control support to validate segmentation, firewalling, and demilitarized zone (DMZ) architecture with minimal operational overhead.
- Reduces the cost and complexity of penetration testing by automating segmentation validation and prioritization.
- Aligns with continuous monitoring and "business as usual" operational practices, helping organizations sustain compliance throughout the year—not just at audit time.

Expanded Testing and Validation

Under PCI DSS 4.0.1, penetration testing and validation requirements are more explicit:

- **Penetration testing** must include both external and internal perspectives, with segmentation tests conducted whenever controls are changed (Req. 11.4).
- Organizations must demonstrate how testing validates the effectiveness of segmentation and other security measures.

RedSeal complements these activities by reducing manual testing burdens, mapping reachable paths, and prioritizing vulnerabilities based on exploitability and business impact.

Strengthened Authentication and Access Controls

PCI DSS 4.0.1 expands requirements for user access:

- **Multi-factor authentication (MFA)** is now required for all access into the CDE (Req. 8.4.2).
- Password policies are strengthened to align with modern authentication best practices (Req. 8.3.6).
- Access reviews must be risk-based and documented (Req. 7.2.5.1).

While RedSeal does not enforce MFA directly, it supports these requirements by validating access paths, identifying unintended connectivity, and highlighting policy gaps that could undermine access controls.

Targeted Risk Analysis

A major innovation in PCI DSS 4.0 is the introduction of **targeted risk analyses**:

- Organizations must **document and perform risk analyses to establish the frequency of specific security activities** (Req. 12.3.1).
- Each analysis must identify the activity in scope, the risk factors considered, and the justification for the chosen frequency.

RedSeal accelerates these analyses by providing a continuously updated model of the environment, correlating vulnerabilities, access paths, and business context to show where risks concentrate.

From PCI DSS 3.2.1 to 4.0.1

PCI DSS 4.0 represented a significant evolution of the standard. PCI DSS 4.0.1, released in 2024, is a **maintenance update** that:

- Provides clarifications, corrected references, and improved consistency across requirements.
- Retains all major enhancements from PCI DSS 4.0.
- Reinforces the Council's emphasis on risk-based, continuous compliance.

Key changes from PCI DSS 3.2.1 → 4.0/4.0.1 include:

- Stronger authentication and password requirements.
- Documented scoping methodology and enhanced segmentation validation.
- Introduction of targeted risk analysis to guide activity frequency.
- More prescriptive penetration testing and vulnerability management requirements.
- Expanded reporting options, including "customized approaches."

The RedSeal Advantage

RedSeal provides organizations with a powerful way to validate network controls and prioritize vulnerabilities under PCI DSS 4.0.1. By analyzing the configuration of network devices and continuously modeling connectivity, RedSeal:

- Ensures segmentation and firewall rules are consistently enforced.
- Identifies deviations and unintended access paths.
- Correlates vulnerabilities with exploitability and business impact, producing prioritized remediation plans.
- Automates the creation of validated network diagrams, inventories, and evidence required for audits.
- Supports continuous monitoring and reporting, directly aligned with PCI DSS 4.0.1's "business as usual" expectations.

No other solution delivers this depth of visibility and efficiency, enabling organizations to sustain PCI compliance while reducing operational overhead.

REDSEAL

Efficient PCI DSS Compliance with RedSeal

RedSeal makes it easier to meet audit and compliance mandates by supporting 42 PCI DSS controls across key areas such as network isolation, firewall validation, and penetration testing. It also automates daily segmentation analysis to sustain “business-as-usual” compliance and can help reduce the size and scope of PCI audits.

PCI CONTROL TYPE	REDSEAL SUPPORT
Network diagram and device inventory	✓
Firewall policy validation	✓
Segmentation validation	✓
Network device configuration hardening	✓
Penetration testing risk prioritization	✓
Business As Usual continuous controls	✓

RedSeal is the only vendor that can implement the continuous network isolation controls required by the PCI DSS in an operationally efficient manner.

RedSeal PCI DSS Control Support Details

Requirement	Sub-Requirements Supported	RedSeal Features
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.2.7, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.2.7, 1.3.1, 1.3.2, 1.3.3, 1.4.1, 1.4.2, 1.4.4	Automated network diagram; access path analysis; PCI network architecture policy validation; network device configuration hardening; best practices validation; maps and views; firewall rule analysis
Requirement 2: Do not use vendor supplied details	2.2.1, 2.2.2, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.3.1, 6.3.1, 6.3.2, 6.3.3, 6.4.1	Network device configuration hardening and best practices validation.
Requirement 6: Develop and maintain secure systems and applications	6.4.2, 6.5.1, 6.5.2, 6.5.3	Risk mapping and prioritization (threat reference library and network connectivity risk assessment); access policy checks; automated policy validation; vulnerabilities and risks; maps and views
Requirement 10: Log and monitor all access to system components and cardholder data.	10.2.1 (only on network devices) 10.6.1 (only on network devices) 10.6.2 (only on network devices)	RedSeal best practice checks and custom best practice checks.
Requirement 11: Regularly test security systems and processes.	11.2.1, 11.2.2, 11.3.1, 11.3.1.1	Automated network segmentation change detection; risk mapping and prioritization; network map
Requirement 12: Support information security with organizational policies and programs	12.5.1 (limited to Host, L2, L3, Device Lists)	Network Inventory, Endpoint inventory, and grouping.
Best Practices/BAU (PCI DSS page 13)	Monitoring of security controls to ensure they are operating effectively and as intended. Ensuring that all failures in security controls are detected and responded to in a timely manner.	RedSeal supports continuous monitoring of the network architecture and scheduled verification of segmentation policy. It also supports continuous prioritization of vulnerabilities to identify risk.

About RedSeal
RedSeal helps organizations see, understand, and secure their hybrid digital environments by uncovering hidden risks, prioritizing exposures, and validating compliance. Trusted by Fortune 1000 companies and U.S. military branches, RedSeal strengthens resilience, streamlines operations, and reduces business risk across IT, remote, OT, cloud, and IoT environments. Visit www.redseal.net.

REDSEAL