SCHNEIDER DOWNS

Big Thinking. Personal Focus.

OUR THOUGHTS ON

PCI DSS v4.0 is Here...Are You Ready?

What do organizations need to know about PCI DSS v4.0?

As entities prepare for their first assessments under the new standard, we want to share some key lessons we've learned while helping our clients prepare to meet the new and changed requirements.

What is PCI DSS?

The PCI DSS is a globally recognized framework that sets technical and operational standards for safeguarding account data.

On March 31, 2022, the PCI Security Standards Council (PCI SSC) released version 4.0 of the PCI DSS, with a three-year transition period for replacing the previous version (3.2.1). This update was intended to address emerging threats, adapt to evolving technologies and introduce innovative ways to combat new risks.

What are the Key Objectives of PCI DSS v4.0?

Continuing to Meet Industry Needs The new version aims to meet the evolving security requirements of the payment industry. It recognizes that security is an ongoing process and adapts accordingly.

Promoting Security as a Continuous Process PCI DSS v4.0 emphasizes that security is not a one-time event but a continuous effort. Organizations must remain vigilant and adapt to changing threats.

Enhancing Flexibility The standard provides flexibility for organizations by introducing additional methods to achieve their security goals. It acknowledges that different approaches can effectively maintain payment.

Improving Payment Validation Methods and Procedures PCI DSS v4.0 enhances validation methods, ensuring that organizations can effectively assess and validate their compliance.

What is the Transition Period and Timeline for PCI DSS v4.0?

Transition Period From March 2022 to March 31, 2024, organizations could operate under both PCI DSS v3.2.1 and v4.0. This allowed time for organizations to familiarize themselves with the changes, update reporting templates and implement necessary adjustments.

Retirement of v3.2.1 As of March 31, 2024, PCI DSS v3.2.1 has been retired, and v4.0 will be the sole active version. Make sure your assessor has completed the mandatory v4.0 training before starting your next assessment.

What are the Key Changes to PCI DSS v4.0?

Over the upcoming month, our team will share insights on some of the more detailed requirement updates and changes to PCI DSS for v4.0, which include:

Requirement 1 - Install and Maintain Network Security Controls The terminology related to firewalls has been revised to encompass a broader range of network security controls. This change supports various technologies used to achieve security objectives traditionally associated with firewalls.

Requirement 2 - Apply Secure Configurations to All System Components There have been several updates designed to clarify the scope and intent of the requirements around securing asset configurations within the cardholder data environment (CDE).

Requirement 3 - Protect Stored Account Data New restrictions have been placed around the storage of sensitive authentication data (SAD), and additional cryptographic controls must be implemented to protect cardholder data (CHD).

Requirement 4 - Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks Trusted keys and certificates must now be formally inventoried.

Requirement 5 - Protect All Systems and Networks from Malicious Software Malware scanning now must cover removable media, and all entities must deploy anti-phishing controls.

Requirement 6 - Develop and Maintain Secure Systems and Software Custom software and client-side scripts used on payment pages must be inventoried, and additional technical controls need to be implemented to protect web-based payment pages.

Requirement 7 - Restrict Access to System Components and Cardholder Data by Business Need to Know User access reviews must be performed at least every six months for all user accounts within the CDE.

Requirement 8 - Identify Users and Authenticate Access to System Components PCI DSS now mandates the implementation of MFA for all access into the cardholder data environment and finally increases minimum password length to 12 characters.

Requirement 9 - Restrict Physical Access to Cardholder Data Only minor changes were made to the restrictions on physical access, both related to additional documentation.

Requirement 10 - Log and Monitor All Access to System Components and Cardholder Data Emphasis is now placed on the use of automation to detect security events, including any failure of all critical security components.

Requirement 11 - Test Security of Systems and Networks Regularly Vulnerability remediation plans must address all severity ratings (not just those considered “high-risk”), and authenticated mode is required for internal vulnerability scans.

Requirement 12 - Support Information Security with Organizational Policies and Programs While additional requirements for documenting responsibilities have been added to Requirements 1-11, the need to perform a full risk assessment (using NIST, OCTAVE, etc.) has been replaced by the Targeted Risk Analysis.

Understanding the Customized Approach in PCI DSS v4.0 Different from the concept of “Compensating Controls” (which still exist), the Customized Approach is only available to entities undergoing an assessment resulting in a Report on Compliance (ROC).

Understanding Targeted Risk Analysis in PCI DSS v4.0 While the Targeted Risk Analysis generally simplifies the risk assessment process, all entities should understand the necessary considerations, especially if incorporating their PCI risk assessment into a broader risk management strategy.

New Requirements for Service Providers Third-party service providers must satisfy additional requirements intended to protect their customers’ PCI environments. Understanding these obligations is equally important to TPSPs and merchants relying on their services.

Be sure to check back to our PCI DSS Solutions page as we make additional guidance and resources available.

How Can Schneider Downs Help?

As a certified Qualified Security Assessor (QSA), Schneider Downs is equipped to assist clients with their PCI compliance requirements by providing scalable, efficient solutions for meeting the rigorous demands of PCI compliance.

If you have any questions regarding PCI DSS v4.0 feel free to contact the Schneider Downs team at **contactsd@schneiderdowns.com** or visit **www.schneiderdowns.com/pcidss**.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

Pittsburgh
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

Columbus
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

Metropolitan Washington
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003