Key Changes in the Payment Card Industry Data Security Standard - PCI DSS v4.0

The PCI Security Standards Council has published version 4.0 of the Payment Card Industry Data Security Standard (PCI DSS) on March 31, 2022.

As a Qualified Security Assessor (QSA), members of the Schneider Downs team were able to review the major revision to the standard prior to release and have collected our thoughts on how the changes will impact entities seeking to maintain compliance under PCI DSS v4.0.

Planning for PCI DSS v4.0

The good news is there are no immediate changes taking effect for most merchants. However, there are new explicit requirements for documentation that were essentially implicit requirements under PCI DSS v3.2.1. Service providers must also provide information to customers regarding which responsibilities fall on the customer and which are handled by the provider.

What is the New Targeted Risk Analysis?

The new phrase, "targeted risk analysis", appears over fifty times in the new PCI DSS publication. The appendix E2 provides a template for evaluating the likelihood of "mischief" (this is the word they chose to describe a negative event). There are eight requirements that ALL entities must complete a targeted risk analysis to determine how the control should be applied to their cardholder data environment (CDE). While this ultimately creates more paperwork for everyone, it does afford some flexibility in control implementation.

What is the New Customized Approach?

While the concept of compensation controls has been a part of PCI DSS for some time, PCI DSS v4.0 introduces the" customized approach". This allows entities to take their own approach to meeting any DSS requirement without the "documented technological or business constraints" required to use the compensating controls approach. Any control met using this approach does require a targeted risk analysis and detailed documentation of the design (effective immediately). One important note is that your QSA cannot assist with control design in order to maintain independence.

Summary of New or Changed Requirements

While most of the new requirements are considered "best practices" until March 2025, there are others that must be implemented effective immediately for any company seeing attestation under PCI DSS v4.0. We recommend companies evaluate all other requirements in the short term and develop a roadmap for implementation over the three-year grace period.

Changes Effective Immediately*

For all Entities

» Roles and responsibilities are now required to be formally documented, assigned, and understood for each of the PCI requirements 1-12.

» **12.5.2 -** PCI scope must be documented and confirmed at least once every 12 months and upon any significant change to the environment.

For service providers only

» **12.9.2 -** Third-party service providers (TPSPs) must provide information to customers regarding their own PCI compliance and a breakdown of customer versus TPSP responsibilities.

Changes Effective March 31, 2025*

For all Entities

Data Management

» **3.2.1 -** Data retention and disposal policies, procedures, and processes must be in place to minimize any SAD stored prior to authorization.

» **3.3.2 -** Any SAD stored electronically prior to authorization must be encrypted using strong cryptography.

» **3.4.2 -** Technical controls must be in place to prevent the copy of primary account numbers (PAN) when using remote-access solutions.

» **3.5.1.1 -** One-time pads are no longer an acceptable means for making PAN unreadable. Hashes used to render PAN unreadable must be keyed cryptographic hashes with appropriate key management.

» **3.5.1.2 –** Disk- and partition-level encryption may only be used to render PAN unreadable on removable media. For non-removable media another mechanism must be used.

» **3.6.1.1 -** All certificates used to encrypt PAN over public networks must be confirmed as valid and not expired or revoked.

» **4.2.1.1 -** An inventory of all trusted keys and certificates must be maintained.

Anti-Malware

» **5.2.3.1 & 5.3.2.1 -** A targeted risk analysis must be performed to determine the frequencies of both:

- Evaluation of systems identified as not at risk for malware
- Frequency of scans on systems running anti-malware

» **5.3.3 -** Malware scans must run when removable media is in use.

» **5.4.1 -** Anti-phishing controls must be in place to protect personnel.

Custom Software & Web Applications

- **6.3.2 -** An inventory of all custom and bespoke software must be maintained.
- **6.4.2 -** An automated technical solution (such as a web application firewall) must be in place to continually detect and prevent web-based attacks.
- **6.4.3 -** Any client-side scripts used on payment pages must be inventoried and integrity-checked.
- **11.6.1 -** Change/tamper detection must be deployed on any web-based payment pages.

Identity & Access Management

- **7.2.4, 7.2.5 & 7.2.5.1 -** User access must be reviewed and validated at least every six months. This applies to both privileged and non-privileged accounts.
- **8.3.6 -** Standard password length must be a minimum of 12 characters. Characters must contain both letters and numbers.
- **8.4.2 & 8.5.1 -** All access to the CDE must be secured using multi-factor authentication (MFA). MFA must be configured to prevent bypass or replay.
- **8.6.1 -** Any interactive logon using system/service accounts must have documented business justification, management approval, and traceability to the individual acting under the system account.
- **8.6.2 -** Passwords for system/service accounts must not be used in hard-coded scripts, configuration files, source code, etc.
- **8.6.3 -** System/service account password length and rotation schedule may be determined based on a targeted risk analysis, but the standard suggests at 15 characters with rotation at least once per year.
- **9.5.1.2.1 -** A targeted risk analysis must be performed to determine the frequency of POI device inspections.

Logging & Alerting

- **10.4.1.1 -** Log reviews must be automated (e.g., through a properly configured SIEM solution) for all critical system components, those that store, process, or transmit cardholder data or SAD, and all security components or appliances.
- **10.4.2.1 -** A targeted risk analysis must be performed to determine the frequency of log reviews for all other systems components.
- **10.7.2 & 10.7.3 -** Prompt detection and response must be in place for all critical security components.
- **A3.3.1 -** Failures of automated log review mechanisms and code review tools must be promptly detected and addressed.

Vulnerability Management

- **11.3.1.1 -** Vulnerability remediation plans must address vulnerabilities rated lower than high or critical.
- **11.3.1.2 -** Internal vulnerability scans must be performed in authenticated mode, with any systems not supporting authenticated scans documented appropriately.

Risk Assessment & Documentation

- **12.3.1 -** A targeted risk analysis must be performed for all controls with flexibility in implementation.
- **12.3.3 -** All cryptographic cipher and protocols in use must be documented, reviewed at least annually, and a documented strategy must be in place for the rapid replacement of any ciphers or protocols found to be vulnerable to compromise.
- **12.3.4 -** Hardware and software technologies in use must be documented and reviewed at least annually to ensure they will continue to be supported by the vendor.

Awareness & Training

- **12.6.2 -** The security awareness program must be reviewed at least annually and updated as needed.
- **12.6.3.1 & 12.6.3.2 -** Awareness training must address threats and vulnerabilities that could impact the security of the CDE, to include at a minimum phishing and other social engineering. Training must also address the acceptable use of end-user technologies.

Incident Response

- **12.10.4.1 -** A targeted risk analysis must be performed to determine the frequency of training for incident response personnel.
- **12.10.5 -** The security incident response plan must account for events from the change/tamper detection on web-based payment pages.
- **12.10.7 -** Specific incident response procedures must be in place to handle the detection of PAN outside the CDE.

Changes for Service Providers Only*

Data Management

- **3.3.3 -** Issuers must store all SAD using strong cryptography.
- **3.6.1.1 -** Documentation and design of the cryptographic environment must prevent the use of the same keys in both production and test environments.

Identity & Access Management

- **8.3.10.1 -** If utilizing passwords/passphrases as a single factor for customer authentication (i.e., no MFA enabled) those passwords must be changed at least every 90 days or "the security posture of accounts is dynamically analyzed to determine real-time access to resources". For further information on the latter option, PCI SSC suggests reading NIST SP 800-207 Zero Trust Architecture.

Penetration Testing

- **11.4.7 -** Third-party hosted/cloud service providers must now support their customers for external penetration testing. This means as a service provider, you must provide evidence of your own penetration test to meet Requirements 11.4.3 and 11.4.4 on the shared infrastructure or allow prompt access to each customer to perform their own penetration test of the infrastructure.

- **A1.1.4 -** Logical separation of the customers' and provider's environments must be confirmed via penetration testing at least once every six months.

Vulnerability Management

- **11.5.1.1 -** Covert malware communication channels (e.g., DNS tunneling) must be addressed via a combination of intrusion detection and prevention techniques. Testing procedures require examination of configuration settings but not tests of effectiveness of the controls.

Risk Assessment & Documentation

- **12.5.2.1 -** The PCI scope must be documented and reviewed every six months (instead of the 12-month cycle established in 12.5.2) and after any significant changes.

- **12.5.3 -** The impact to PCI compliance of any significant organizational changes must be documented and reported to executive management.

- **A1.1.1 -** Logical separation must be established between the customers' and provider's environments.

- **A1.2.3 -** The provider must implement mechanisms for customers to securely report suspected incidents and vulnerabilities to the provider.

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 4.0 feel free to contact the Schneider Downs team at contactsd@schneiderdowns.com or visit our PCI DSS solutions website.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

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

WASHINGTON, D.C.
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003

*Source: Securing the Future of Payments: PCI SSC Publishes PCI Data Security Standard v4.0 (pcisecuritystandards.org)