WHITE PAPER

PCI DSS 4.0 Changes: A List of the New Requirements

The time for the transition from PCI DSS 3.2.1 to 4.0 has arrived.

JUSTIN BONK, CISSP, PCI-QSA, CIPP / US, CIA, CFE, CISA
SENIOR MANAGER, RISK ADVISORY SERVICES

It's time to begin your organization's transition from PCI DSS 3.2.1 to PCI DSS 4.0, but it's not going to be that bad. If your organization is current with PCI 3.2.1 compliance requirements, transitioning to 4.0 should not be a difficult move.

There are 64 new requirements. Of those:

13 need to be met up front for any PCI DSS 4.0 assessment.

Of those 13, 10 deal directly with formally defining roles and responsibilities for requirements and the remaining 3 should not be considered onerous or costly to implement.

The remaining 51 new requirements become effective March 31, 2025, leaving you with time to determine your approach and implement controls and processes where necessary.

See my blog post, "PCI DSS 4.0 Compliance Will Not Be as Onerous or Costly as You Might Think" for a deeper dive on these requirements and an assessment of their implementation challenges.

A Listing of the New PCI DSS 4.0 Requirements

REQ #	REQUIREMENT
2.1.2	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood
3.1.2	Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood
3.2.1	Any SAD stored prior to completion of authorization is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes
3.3.2	SAD stored electronically prior to completion of authorization is encrypted using strong cryptography
3.3.3	SAD stored by issuers is encrypted using strong cryptography
3.4.2	Technical controls to prevent copy and / or relocation of PAN when using remote-access technologies except with explicit authorization
3.5.1.1	Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN with associated key-management processes and procedures
3.5.1.2	Implementation of disk-level or partition-level encryption when used to render PAN unreadable
3.6.1.1	A documented description of the cryptographic architecture includes prevention of the use of cryptographic keys in production and test environments
4.1.2	Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood
4.2.1	Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked
4.2.1.1	An inventory of the entity’s trusted keys and certificates is maintained
5.1.2	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood
5.2.3.1	A targeted risk analysis is performed to determine frequency of periodic evaluations of system components identified as not at risk for malware
5.3.2.1	A targeted risk analysis is performed to determine frequency of periodic malware scans
5.3.3	Anti-malware scans are performed when removable electronic media is in use

REQ #	REQUIREMENT
5.4.1	Mechanisms are in place to detect and protect personnel against phishing attacks
6.1.2	Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood
6.3.2	Maintain an inventory of bespoke and custom software to facilitate vulnerability and patch management
6.4.2	Deploy an automated technical solution for public-facing web applications that continually detects and prevents web-based attacks
6.4.3	Manage all payment page scripts that are loaded and executed in the consumer's browser
7.1.2	Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood
7.2.4	Review all user accounts and related access privileges appropriately
7.2.5	Assign and manage all application and system accounts and related access privileges appropriately
7.2.5.1	Review all access by application and system accounts and related access privileges
8.1.2	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood
8.3.6	Minimum level of complexity for passwords when used as an authentication factor
8.3.10.1	If passwords / passphrases are the only authentication factor for customer user access, passwords / passphrases are changed at least every 90 days or the security posture of accounts is dynamically analyzed to determine real-time access to resources
8.4.2	Multi-factor authentication for all access into the CDE
8.5.1	Multi-factor authentication systems are implemented appropriately
8.6.1	Manage interactive login for accounts used by systems or applications
8.6.2	Passwords / passphrases used for interactive login for application and system accounts are protected against misuse
8.6.3	Passwords / passphrases for any application and system accounts are protected against misuse
9.1.2	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood
9.5.1.2.1	A targeted risk analysis is performed to determine frequency of periodic POI device inspections

REQ #	REQUIREMENT
10.1.2	Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood
10.4.1.1	Audit log reviews are automated
10.4.2.1	A targeted risk analysis is performed to determine frequency of log reviews for all other system components
10.7.2	Failures of critical security control systems are detected, alerted, and addressed promptly
10.7.3	Failures of critical security control systems are responded to promptly
11.1.2	Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood
11.3.1.1	Manage all other applicable vulnerabilities (those not ranked as high-risk or critical)
11.3.1.2	Internal vulnerability scans are performed via authenticated scanning
11.4.7	Multi-tenant service providers support their customers for external penetration testing
11.5.1.1	Covert malware communication channels detect, alert and / or prevent, and address via intrusion-detection and / or intrusion-prevention techniques
11.6.1	A change-and-tamper-detection mechanism is deployed for payment pages
12.3.1	A targeted risk analysis is documented to support each PCI DSS requirement that provides flexibility for how frequently it is performed
12.3.2	A targeted risk analysis is performed for each PCI DSS requirement that is met with the customized approach
12.3.3	Cryptographic cipher suites and protocols in use are documented and reviewed
12.3.4	Hardware and software technologies are reviewed
12.5.2	PCI DSS scope is documented and confirmed at least once every 12 months
12.5.2.1	PCI DSS scope is documented and confirmed at least once every six months and upon significant changes (service providers)
12.5.3	The impact of significant organizational changes on PCI DSS scope is documented and reviewed and results are communicated to executive management
12.6.2	The security awareness program is reviewed at least once every 12 months and updated as needed

REQ #	REQUIREMENT
12.6.3.1	Security awareness training includes awareness of threats that could impact the security of the CDE, to include phishing and related attacks and social engineering
12.6.3.2	Security awareness training includes awareness about acceptable use of end-user technologies
12.9.2	TPSPs support customers' requests to provide PCI DSS compliance status and information about PCI DSS requirements that are the responsibility of the TPSP
12.10.4.1	A targeted risk analysis is performed to determine frequency of periodic training for incident response personnel
12.10.5	The security incident response plan includes alerts from the change- and tamper-detection mechanism for payment pages
12.10.7	Incident response procedures are in place and initiated upon detection of PAN
A1.1.1	The multi-tenant service provider confirms access to and from customer environment is logically separated to prevent unauthorized access
A1.1.4	The multi-tenant service provider confirms effectiveness of logical separation controls used to separate customer environments at leave once every six months via penetration testing
A1.2.3	The multi-tenant service provider implements processes or mechanisms for reporting and addressing suspected or confirmed security incidents and vulnerabilities
A3.3.1	Failures of the following are detected, alerted, and reported in a timely manner: • Automated log review mechanisms • Automated code review tools

Questions on the new PCI DSS 4.0 Changes and Compliance Requirements?

Contact me for a discussion of your PCI compliance situation and approaches for meeting deadlines required by PCI 4.0. You can reach me at justin.bonk@freedmaxick.com or 716.332.2680.

Trust earned.
FreedMaxick®