LinkedIn Naved Anjum

PCI Security Standards Council®

Summary of Changes

VERSION 3.2.1 TO 4.0

Requirements	PCI DSS 4.0	PCI DSS 3.2.1
1. Install and Maintain Network Security Controls	• Roles and responsibilities must be documented, assigned, and understood	• No explicit requirement for documented roles and responsibilities
2. Apply Secure Configurations to All System Components	• Roles and responsibilities must be documented, assigned, and understood	• No explicit requirement for documented roles and responsibilities
3. Protect Stored Account Data	• Roles and responsibilities must be documented • New requirement for storage of SAD by issuers • New data retention policies for SAD stored prior to authorization • Must encrypt SAD stored electronically prior to authorization • Technical controls to prevent PAN copying during remote access • Requires keyed cryptographic hashes • Specific requirements for disk-level encryption • Service providers must prevent use of same cryptographic keys in production and test	• Less specific requirements for SAD storage and encryption • No specific requirements for cryptographic hashing methods • No distinction between production and test environment keys

Requirement	PCI DSS 4.0	PCI DSS 3.2.1
4. Protect Cardholder Data with Strong Cryptography During Transmission	• Roles and responsibilities must be documented • Must validate certificates for PAN transmission • Must maintain inventory of trusted keys and certificates	• No explicit requirements for certificate validation • No requirement for key and certificate inventory
5. Protect All Systems from Malicious Software	• Roles and responsibilities must be documented • Risk-based evaluation of systems not at risk for malware • Risk-based periodic malware scans • Malware solution for removable media • Must detect and protect against phishing attacks	• Less comprehensive malware protection requirements • No specific requirements for phishing protection • No explicit requirements for removable media
6. Develop and Maintain Secure Systems and Software	• Roles and responsibilities must be documented • Must maintain inventory of bespoke and custom software • Mandatory automated solution for public-facing web applications • Management of payment page scripts	• Manual or automated web application assessment allowed • No explicit requirement for software inventory • Less specific requirements for payment page scripts
7. Restrict Access by Business Need to Know	• Roles and responsibilities must be documented • Review of all user accounts and access privileges • Management of application and system accounts • Review of application and system account access	• Less specific requirements for access review • No explicit requirements for application and system account management
8. Identify Users and Authenticate Access	• Roles and responsibilities must be documented • 10 invalid attempts before lockout • 12-character minimum password length • MFA for all CDE access • Secure MFA implementation • Management of interactive login accounts	• 6 invalid attempts before lockout • 7-character minimum password length • MFA only required for remote access • Less specific requirements for account management

Requirement	PCI DSS 4.0	PCI DSS 3.2.1
9. Restrict Physical Access	• Roles and responsibilities must be documented • Console locking in sensitive areas • Risk-based POI device inspections	• No specific requirements for console locking • Less structured approach to POI device inspections
10. Log and Monitor All Access	• Roles and responsibilities must be documented • Automated log review mechanisms • Risk-based periodic log reviews • Detection and response to security control failures	• Manual log review processes acceptable • Less specific requirements for security control monitoring
11. Test Security Systems and Processes	• Roles and responsibilities must be documented • Management of all vulnerabilities • Authenticated internal vulnerability scans • Payment page tampering detection • Service providers must support customer penetration testing • Intrusion detection/prevention for malware channels	• Less comprehensive vulnerability management requirements • No specific requirements for authenticated scanning • Less specific requirements for intrusion detection
12. Maintain Security Policies	• Formal acknowledgement of responsibilities • Risk analysis for customized approaches • Regular scope documentation • Annual review of technologies • Enhanced security awareness program • Incident response for unexpected PAN storage • Service provider specific requirements	• Less formal requirements for policy management • Less specific requirements for security awareness • No specific requirements for unexpected PAN storage • Fewer service provider-specific requirements

PCI DSS v4.0 Transition Timeline