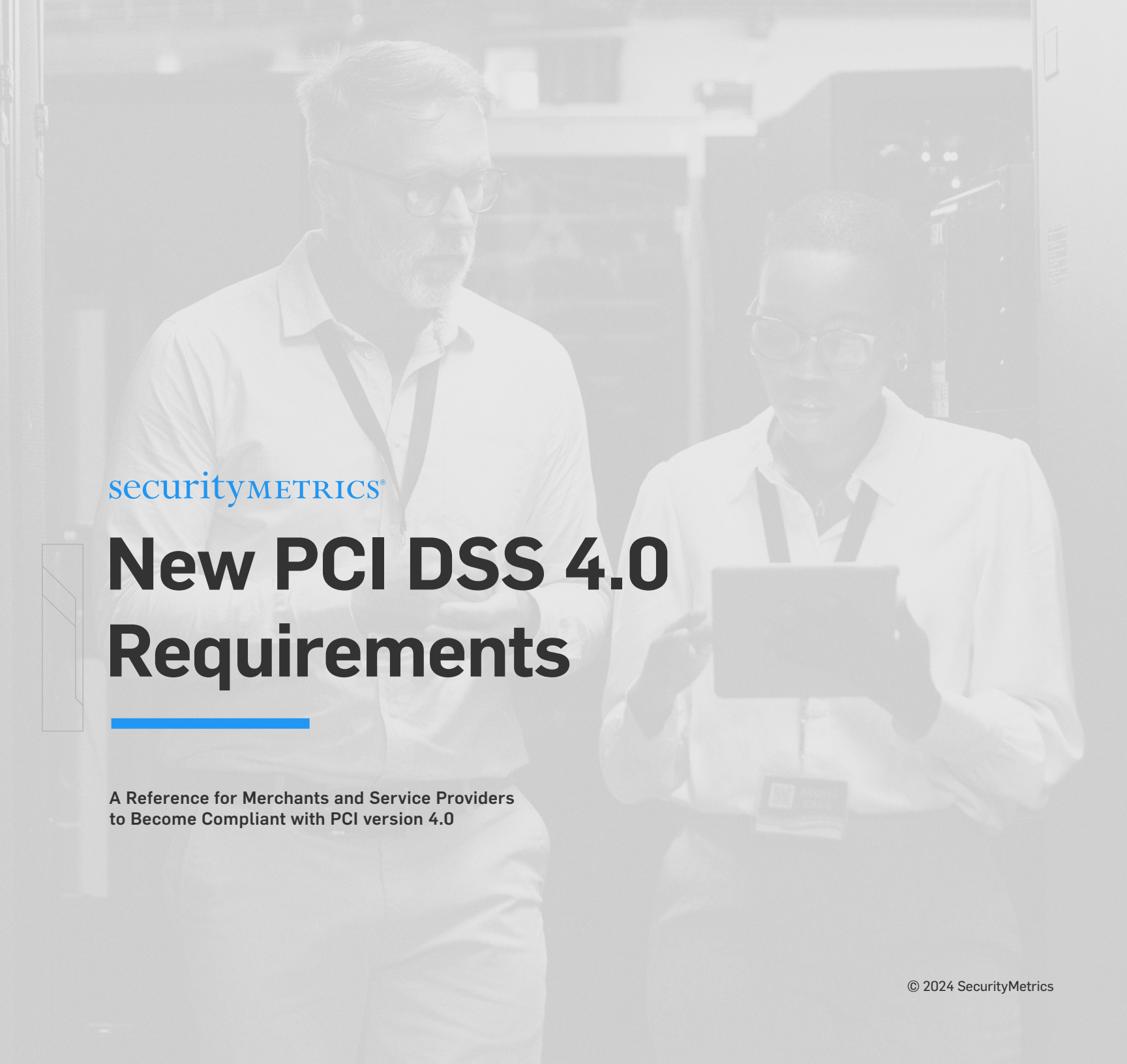


securityMETRICS®

New PCI DSS 4.0 Requirements

A Reference for Merchants and Service Providers to Become Compliant with PCI version 4.0

NEW PCI DSS 4.0 REQUIREMENTS

NEW REQ.	SAQ TYPE		Effective Immediately	Effective March 31, 2025
REQUIREMENT 1: APPLY SECURE CONFIGURATIONS TO ALL SYSTEM COMPONENTS				
1.1.2	D (Mer), D (SP)	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	■	
REQUIREMENT 2: APPLY SECURE CONFIGURATIONS TO ALL SYSTEM COMPONENTS				
2.1.2	D (Mer), D (SP)	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	■	
REQUIREMENT 3: PROTECT STORED ACCOUNT DATA				
3.1.2	D (Mer), D (SP)	Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	■	
3.2.1	A, A-EP, D (Mer), D (SP), P2PE	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	D (Mer), D (SP)	SAD stored electronically prior to completion of authorization is encrypted using strong cryptography.		■
3.3.3	D (SP)	SAD stored by issuers is encrypted using strong cryptography.		■
3.4.2	D (Mer), D (SP)	Technical controls to prevent copy and/or relocation of PAN when using remote-access technologies except with explicit authorization.		■
3.4.2	D (Mer), D (SP)	Technical controls to prevent copy and/or relocation of PAN when using remote-access technologies except with explicit authorization.		■
3.5.1.1	D (Mer), D (SP)	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 keymanagement processes and procedures.		■
3.5.1.2	D (Mer), D (SP)	Implementation of disk-level or partitionlevel encryption when used to render PAN unreadable.		■

NEW REQ.	SAQ TYPE		Effective Immediately	Effective March 31, 2025
3.6.1.1	D (SP)	A documented description of the cryptographic architecture includes prevention of the use of cryptographic keys in production and test environments.		■
REQUIREMENT 4: PROTECT CARDHOLDER DATA WITH STRONG CRYPTOGRAPHY DURING TRANSMISSION OVER OPEN, PUBLIC NETWORKS				
4.1.2	A-EP, D (Mer), D (SP)	Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	■	
4.2.1	C, D (Mer), D (SP)	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	D (Mer.), D (SP)	An inventory of the entity's trusted keys and certificates is maintained.		■
REQUIREMENT 5: PROTECT ALL SYSTEMS AND NETWORKS FROM MALICIOUS SOFTWARE				
5.1.2	D (Mer), D (SP)	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	■	
5.2.3.1	A-EP, C, D (Mer), D (SP)	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-EP, C, D (Mer), D (SP)	A targeted risk analysis is performed to determine frequency of periodic malware scans.		■
5.3.3	A-EP, C, C-VT, D (Mer), D (SP)	Anti-malware scans are performed when removable electronic media is in use.		■
5.4.1	A-EP, C, C-VT, D (Mer), D (SP)	Mechanisms are in place to detect and protect personnel against phishing attacks.		■
REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND SOFTWARE				
6.1.2	D (Mer), D (SP)	Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	■	

NEW REQ.	SAQ TYPE		Effective Immediately	Effective March 31, 2025
6.3.2	A-EP, D (Mer.), D (SP)	Maintain an inventory of bespoke and custom software to facilitate vulnerability and patch management.		■
6.3.2	A-EP, D (Mer), D (SP)	Maintain an inventory of bespoke and custom software to facilitate vulnerability and patch management.		■
6.4.2	A-EP, D (Mer), D (SP)	Deploy an automated technical solution for public-facing web applications that continually detects and prevents webbased attacks.		■
6.4.3	A, A-EP, D (Mer), D (SP)	Manage all payment page scripts that are loaded and executed in the consumer's browser.		■
REQUIREMENT 7: RESTRICT ACCESS TO SYSTEM COMPONENTS AND CARDHOLDER DATA BY BUSINESS NEED TO KNOW				
7.1.2	D (Mer), D (SP)	Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	■	
7.2.4	A-EP, C, D (Mer), D (SP)	Review all user accounts and related access privileges appropriately.		■
7.2.5	A-EP, C, D (Mer), D (SP)	Assign and manage all application and system accounts and related access privileges appropriately.		■
7.2.5.1	D (Mer), D (SP)	Review all access by application and system accounts and related access privileges.		■
REQUIREMENT 8: IDENTIFY USERS AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS				
8.1.2	D (Mer), D (SP)	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	■	
8.3.6	A, A-EP, C, C-VT, D (Mer), D (SP)	Minimum level of complexity for passwords when used as an authentication factor.		■

NEW REQ.	SAQ TYPE		Effective Immediately	Effective March 31, 2025
8.3.10.1	D (SP)	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 realtime access to resources.		■
8.4.2	A-EP, C, D (Mer), D (SP)	Multi-factor authentication for all access into the CDE.		■
8.5.1	A-EP, C, D (Mer), D (SP)	Multi-factor authentication systems are implemented appropriately.		■
8.6.1	A-EP, C, D (Mer), D (SP)	Manage interactive login for accounts used by systems or applications.		■
8.6.2	A-EP, C, D (Mer), D (SP)	Passwords/passphrases used for interactive login for application and system accounts are protected against misuse.		■
8.6.3	A-EP, C, D (Mer), D (SP)	Passwords/passphrases for any application and system accounts are protected against misuse.		■
REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA				
9.1.2	D (Mer), D (SP)	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	■	
9.5.1.2.1	D (Mer), D (SP)	A targeted risk analysis is performed to determine frequency of periodic POI device inspections.		■
REQUIREMENT 10: LOG AND MONITOR ALL ACCESS TO SYSTEM COMPONENTS AND CARDHOLDER DATA				
10.1.2	D (Mer), D (SP)	Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	■	
10.4.1.1	A-EP, C, D (Mer), D (SP)	Audit log reviews are automated.		■
10.4.2.1	A-EP, C, D (Mer), D (SP)	A targeted risk analysis is performed to determine frequency of log reviews for all other system components.		■

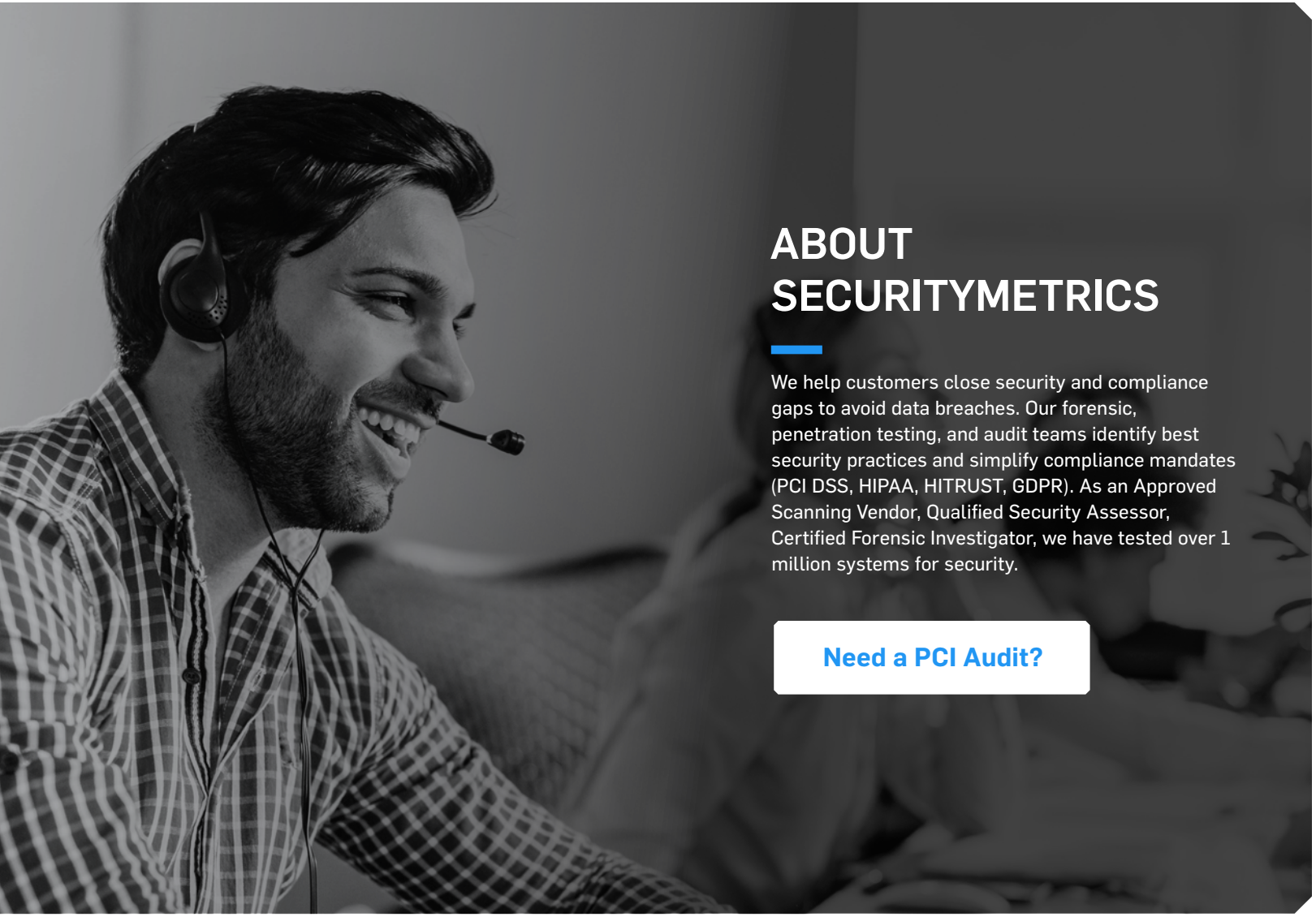
NEW REQ.	SAQ TYPE		Effective Immediately	Effective March 31, 2025
10.7.2	D (Mer), D (SP)	Failures of critical security control systems are detected, alerted, and addressed promptly.		■
10.7.3	D (Mer), D (SP)	Failures of critical security control systems are responded to promptly.		
REQUIREMENT 11: TEST SECURITY OF SYSTEMS AND NETWORKS REGULARLY				
11.1.2	D (Mer), D (SP)	Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	■	
11.3.1.1	D (Mer), D (SP)	Manage all other applicable vulnerabilities (those not ranked as highrisk or critical).		■
11.3.1.2	D (Mer), D (SP)	Internal vulnerability scans are performed via authenticated scanning.		■
11.3.2	A*, A-EP, B-IP, C, D (Mer), D (SP)	External vulnerability scans are performed at least quarterly by a PCI SSC Approved Scanning Vendor (ASV) and that vulnerabilities are resolved per the ASV Program Guide.	■	
11.4.7	D (SP)	Multi-tenant service providers support their customers for external penetration testing.		■
11.5.1.1	D (SP)	Covert malware communication channels detect, alert and/or prevent, and address via intrusion-detection and/or intrusion-prevention techniques.		■
11.6.1	A, A-EP, D (Mer), D (SP)	A change-and-tamper-detection mechanism is deployed for payment pages.		■
REQUIREMENT 12: SUPPORT INFORMATION SECURITY WITH ORGANIZATIONAL POLICIES AND PROGRAMS				
12.3.1	A-EP, C, D (Mer), D (SP)	A targeted risk analysis is documented to support each PCI DSS requirement that provides flexibility for how frequently it is performed.		■
12.3.2	D (Mer), D (SP)	A targeted risk analysis is performed for each PCI DSS requirement that is met with the customized approach.	■	

*This requirement is only new for SAQ A.

NEW REQ.	SAQ TYPE		Effective Immediately	Effective March 31, 2025
12.3.3	D (Mer), D (SP)	Cryptographic cipher suites and protocols in use are documented and reviewed.		■
12.3.4	D (Mer), D (SP)	Hardware and software technologies are reviewed.		■
12.5.2	D (Mer), D (SP)	PCI DSS scope is documented and confirmed at least once every 12 months.	■	
12.5.2.1	D (SP)	PCI DSS scope is documented and confirmed at least once every six months and upon significant changes.		■
12.5.3	D (SP)	The impact of significant organizational changes on PCI DSS scope is documented and reviewed and results are communicated to executive management.		■
12.6.2	D (Mer), D (SP)	The security awareness program is reviewed at least once every 12 months and updated as needed.		■
12.6.3.1	A-EP, C, C-VT, D (Mer), D (SP)	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	D (Mer), D (SP)	Security awareness training includes awareness about acceptable use of enduser technologies.		■
12.9.2	D (SP)	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	D (Mer), D (SP)	A targeted risk analysis is performed to determine frequency of periodic training for incident response personnel.		■
12.10.5	D (Mer), D (SP)	The security incident response plan includes alerts from the change- and tamper-detection mechanism for payment pages.		■

NEW REQ.	SAQ TYPE		Effective Immediately	Effective March 31, 2025
12.10.7	D (Mer), D (SP)	Incident response procedures are in place and initiated upon detection of PAN.		
APPENDIX A1: ADDITIONAL PCI DSS REQUIREMENTS FOR MULTI-TENANT SERVICE PROVIDERS				
A1.1.1	D (SP)	The multi-tenant service provider confirms access to and from customer environment is logically separated to prevent unautho-rized access.		
A1.1.4	D (SP)	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	D (SP)	The multi-tenant service provider implements processes or mechanisms for reporting and addressing suspected or confirmed security incidents and vulnerabilities.		
APPENDIX A3: DESIGNATED ENTITIES SUPPLEMENTAL VALIDATION (DESV)				
A3.3.1	Entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements	Failures of the following are detected, alerted, and reported in a timely manner: Automated log review mechanisms Automated code review tools		
TOTALS			13	51
GRAND TOTAL: 64				

*Immediately for All v4.0 Assessments



ABOUT SECURITYMETRICS

We help customers close security and compliance gaps to avoid data breaches. Our forensic, penetration testing, and audit teams identify best security practices and simplify compliance mandates (PCI DSS, HIPAA, HITRUST, GDPR). As an Approved Scanning Vendor, Qualified Security Assessor, Certified Forensic Investigator, we have tested over 1 million systems for security.

Need a PCI Audit?