PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) V4.0

PCI DSS Version 4.0 New Requirements

V4.0 OF THE DATA SECURITY STANDARDS

The Payment Card Industry Security Standards Council (PCI SSC) released V.0 of the PCI Data Security Standards (PCI DSS) on March 31, 2022. With version 3.2.1 being retired on March 31, 2024, there will be a yearlong period when some V4.0 standards become mandatory and others are treated as guidelines, until they also become mandatory standards after March 31, 2025. As the timeframe for transition approaches, it's important to understand what has changed in PCI DSS V4.0.

FUTURE DATED REQUIREMENTS

PCI V4.0 includes future dated new requirements and testing procedures. These future dated new requirements are designated as best practice until March 31, 2025. After March 31, 2025, the future dated new requirements become mandatory and must be considered during an organization's PCI DSS assessment.

TIMELINE AT A GLANCE

Here is a summary of the important implementation timeline dates for PCI V4.0:

- PCI V4.0 was released on March 31, 2022.
- Transition period is from March 31, 2022, through March 31, 2024. The transition period is the period where an organization's Cardholder Data Environment (CDE) can be assessed using PCI DSS v3.2.1 or V4.0.
- PCI v3.2.1 retires on March 31, 2024. After this date, V4.0 is mandatory.
- Future dated new requirements are mandatory after March 31, 2025.

NEW REQUIREMENTS FOR V4.0

As with previous releases of PCI DSS, most of the changes in V4.0 are future dated. This means the future-dated requirements are a recommended best practice until March 31, 2025. At this time, all future-dated requirements will be mandatory. In addition to new requirements, the PCI Council made numerous changes to the requirements in V4.0. These changes are referred to as evolving requirement, clarification or guidance, and structure or format.

- Evolving requirements
  - New requirements
  - Updated requirements or testing procedures
  - Deleted requirements
- Clarification or guidance
  - Aligning the requirement and the testing procedure
  - Clearer wording and applicability notes
  - New appendices D and E for assessments using the new customized approach
- Structure or format
  - Combining, moving and renumbering requirements

The following content focuses on "evolving requirements," as these incorporate the new requirements organizations will be required to implement when being assessed against V4.0. Future-dated requirements will be noted below as well.

REQUIREMENT 1

Install and Maintain Network Security Controls. Processes and mechanisms for installing and maintaining security controls are defined and understood.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
1.1.2	The roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	X		X	

REQUIREMENT 2

Apply Secure Configurations to All System Components. Processes and mechanisms for applying secure configurations to all system components are defined and understood.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
2.1.2	The roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	X		X	

REQUIREMENT 3

Protect Stored Account Data. Processes and mechanisms for protecting stored account data are defined and understood.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
3.1.2	The roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	X		X	
3.2.1	New requirement. A sub-requirement has been added to an existing requirement to address SAD stored prior to completion of authorization through implementation of data retention and disposal policies, procedures, and processes.	X			X
3.3.2	New requirement to encrypt SAD that is stored electronically prior to completion of authorization.	X			X

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
3.3.3	New requirement to address former testing procedures that any storage of SAD by issuers is limited to that which is needed for a legitimate issuing business need and is secured.	X		X	
3.4.2	New requirement for technical controls to prevent copy and/or relocation of PAN when using remote-access technologies. Expanded from former Requirement 12.3.10.	X			X
3.5.1.1	New requirement for keyed cryptographic hashes when hashing is used to render PAN unreadable.	X			X
3.5.1.2	New requirement that disk-level or partition-level encryption is used only to render PAN unreadable on removable electronic media or, if used on non-removable electronic media, the PAN is also rendered unreadable via a mechanism that meets Requirement 3.5.1.	X			X
3.6.1.1	New requirement. A sub-requirement has been added to an existing requirement to maintain a documented description of the cryptographic architecture that includes prevention of the use of the same cryptographic keys in production and test environments.		X		X

REQUIREMENT 4

Protect Cardholder Data With Strong Cryptography During Transmission Over Open, Public Networks. Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
4.1.2	The roles and responsibilities for performing activities in requirement 4 are documented, assigned, and understood.	X		X	
4.2.1	New requirement. A sub-requirement has been added to an existing requirement to confirm certificates used for PAN transmissions over open, public networks are valid and not expired or revoked.	X			X
4.2.1.1	New requirement to maintain an inventory of trusted keys and certificates.	X			X

REQUIREMENT 5

Protect All Systems and Networks From Malicious Software. Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
5.1.2	The roles and responsibilities for performing activities in requirement 5 are documented, assigned, and understood.	X		X	
5.2.3.1	New requirement to define the frequency of periodic evaluations of system components not at risk for malware in the entity's targeted risk analysis.	X			X
5.3.2.1	New requirement to define the frequency of periodic malware scans in the entity's targeted risk analysis.	X			X
5.3.3	New requirement for a malware solution for removable electronic media.	X			X
5.4.1	New requirement to detect and protect personnel against phishing attacks.	X			X

REQUIREMENT 6

Develop and Maintain Secure Systems and Software. Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
6.1.2	The roles and responsibilities for performing activities in requirement 6 are documented, assigned, and understood.	X		X	
6.3.2	New requirement to maintain an inventory of bespoke and custom software.	X			X
6.4.2	New requirement to deploy an automated technical solution for public-facing web applications that continually detects and prevents web-based attacks. This new requirement removes the option in Requirement 6.4.1 to review web applications via manual or automated application vulnerability assessment tools or methods.	X			X
6.4.3	New requirement for management of all payment page scripts that are loaded and executed in the consumer's browser.	X			X

REQUIREMENT 7

Restrict Access to System Components and Cardholder Data by Business Need to Know. 7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
7.1.2	The roles and responsibilities for performing activities in requirement 7 are documented, assigned, and understood.	X		X	
7.2.4	New requirement for review of all user accounts and related access privileges.	X			X
7.2.5	New requirement for assignment and management of all application and system accounts and related access privileges.	X			X
7.2.5.1	New requirement for review of all access by application and system accounts and related access privileges.	X			X

REQUIREMENT 8

Identify Users and Authenticate Access to System Components. Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
8.1.2	The roles and responsibilities for performing activities in requirement 8 are documented, assigned, and understood.	X		X	
8.3.4	Increased the number of invalid authentication attempts before locking out a user ID from six to ten attempts.	X		X	

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
8.3.6	New requirement to increase password length from a minimum length of seven characters to minimum length of 12 characters (or if the system does not support 12 characters, a minimum length of eight characters). Clarified that, until March 31 2025, passwords must be a minimum length of at least seven characters in accordance with v3.2.1 Requirement 8.2.3. Clarified that this requirement applies only if passwords/passphrases are used as an authentication factor to meet Requirement 8.3.1. Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	X			X
8.3.9	Added the option to determine access to resources automatically by dynamically analyzing the security posture of accounts, instead of changing passwords/passphrases at least once every 90 days.	X		X	
8.3.10.1	New requirement - if passwords/passphrases are the only authentication factor for customer user access, then passwords/passphrases are either changed at least once every 90 days or access to resources is automatically determined by dynamically analyzing the security posture of the accounts.	X			X
8.4.2	New requirement to implement multi-factor authentication (MFA) for all access into the CDE.	X			X
8.5.1	New requirement for secure implementation of multi-factor authentication systems.	X			X
8.6.1	New requirement for management of system or application accounts that can be used for interactive login.	X			X
8.6.2	New requirement for not hard-coding passwords/passphrases into files or scripts for any application and system accounts that can be used for interactive login.	X			X
8.6.3	New requirement for protecting passwords/passphrases for application and system accounts against misuse.	X			X

REQUIREMENT 9

Restrict Physical Access to Cardholder Data. Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
9.1.2	The roles and responsibilities for performing activities in requirement 9 are documented, assigned, and understood.	X		X	
9.2.4	New requirement. A sub-requirement has been added to an existing requirement to restrict access to consoles in sensitive areas via locking when not in use.	X		X	
9.5.1.2.1	New requirement to define the frequency of periodic POI device inspections based on the entity's targeted risk analysis.	X			X

REQUIREMENT 10

Log and Monitor All Access to System Components and Cardholder Data. Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
10.1.2	The roles and responsibilities for performing activities in requirement 10 are documented, assigned, and understood.	X		X	
10.4.1.1	New requirement for the use of automated mechanisms to perform audit log reviews.	X			X
10.4.2.1	New requirement for a targeted risk analysis to define the frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1).	X			X
10.7.2	New requirement for all entities to detect, alert, and promptly address failures of critical security control systems. This requirement applies to all entities – it includes two additional critical security controls not included in Requirement 10.7.1 for service providers.	X			X
10.7.3	New requirement to respond promptly to failures of any critical security controls. For service providers: this is a current PCI DSS v3.2.1 requirement. For all other (non-service provider) entities: this is a new requirement.	X			X

REQUIREMENT 11

Test Security of Systems and Networks Regularly. Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
11.1.2	The roles and responsibilities for performing activities in requirement 11 are documented, assigned, and understood.	X		X	
11.3.1.1	New requirement to manage all other applicable vulnerabilities (those not ranked as high-risk or critical) found during internal vulnerability scans.	X			X
11.3.1.2	New requirement to perform internal vulnerability scans via authenticated scanning.	X			X
11.4.7	New requirement for multi-tenant service providers to support their customers for external penetration testing.		X		X
11.5.1.1	New requirement to use intrusion-detection and or intrusion-prevention techniques to detect, alert on/prevent, and address covert malware communication channels.		X		X
11.6.1	New requirement to deploy a change-and-tamper-detection mechanism to alert for unauthorized modifications to the HTTP headers and contents of payment pages as received by the consumer browser.	X			X

REQUIREMENT 12

Support Information Security with Organizational Policies and Programs. A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
12.1.3	Added formal acknowledgment by personnel of their responsibilities.	X		X	
12.3.1	New requirement to perform a targeted risk analysis for any PCI DSS requirement that provides flexibility for how frequently it is performed.	X			X
12.3.2	New requirement for entities using a Customized Approach to perform a targeted risk analysis for each PCI DSS requirement that the entity meets with the customized approach.	X		X	

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
12.3.3	New requirement to document and review cryptographic cipher suites and protocols in use at least once every 12 months.	X			X
12.3.4	New requirement to review hardware and software technologies in use at least once every 12 months.	X			X
12.5.2	New requirement to document and confirm PCI DSS scope at least every 12 months and upon significant change to the in-scope environment.	X		X	
12.5.2.1	New requirement for service providers to document and confirm PCI DSS scope at least once every six months and upon significant change to the in-scope environment.		X		X
12.5.3	New requirement for service providers for a documented review of the impact to PCI DSS scope and applicability of controls upon significant changes to organizational structure.		X		X
12.6.2	New requirement to review and update (as needed) the security awareness program at least once every 12 months.	X			X
12.6.3.1	New requirement for security awareness training to include awareness of threats and vulnerabilities that could impact the security of the CDE.	X			X
12.6.3.2	New requirement for security awareness training to include awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.	X			X
12.8.5	Clarified that the information about PCI DSS requirements managed by the TPSP and the entity should include any that are shared between the TPSP and the entity.	X		X	
12.9.2	New requirement to support customers' requests for information to meet Requirements 12.8.4 and 12.8.5.		X	X	
12.10.4.1	New requirement to perform a targeted risk analysis to define the frequency of periodic training for incident response personnel.	X			X

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
12.10.5	Merged requirements and updated the security monitoring systems to be monitored and responded to as part of the incident response plan to include the following: Detection of unauthorized wireless access points (former 11.1.2), Change-detection mechanism for critical files (former 11.5.1), New requirement. A sub-requirement has been added to an existing requirement for use of a change- and tamper-detection mechanism for payment pages (relates to new requirement 11.6.1).	X			X
12.10.7	New requirement for incident response procedures to be in place and initiated upon detection of stored PAN anywhere it is not expected.	X			X

APPENDIX A1

Additional PCI DSS Requirements for Multi-Tenant Service Providers. Multi-tenant service providers protect and separate all customer environments and data.

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
A1.1.1	New requirement for to implement logical separation between providers' environments and customers' environments.	X			X
A1.1.4	New requirement to confirm, via penetration testing, the effectiveness of logical separation controls used to separate customer environments.	X			X
A1.2.3	New requirement for the implementation of processes and mechanisms for reporting and addressing suspected or confirmed security incidents and vulnerabilities.	X			X

APPENDIX A3

NEW REQUIREMENT		APPLICABLE TO		EFFECTIVE DATE	
		All Entities	Service Providers Only	Immediately for all V4.0 Assessments	March 31, 2025
A3.3.1	New requirement. A sub-requirement has been added to an existing requirement to detect, alert, and report failures of automated log review mechanisms.	X			X
A3.3.1	New requirement. A sub-requirement has been added to an existing requirement to detect, alert, and report failures of automated code review tools.	X			X

BDO USA Can Help

As a Qualified Security Assessor Company (QSAC), BDO USA has experienced QSAs who can assist your organization in understanding and transitioning to the new PCI V4.0 standards.

HAVE QUESTIONS OR WANT TO LEARN MORE? CONTACT US!

GREG SCHU
Cybersecurity, Compliance, and Assessments Services Principal
gschu@bdo.com

BRIAN HILL
Cybersecurity, Compliance, and Assessments Services Managing Director
bhill@bdo.com

FRED BRANTNER
Cybersecurity, Compliance, and Assessments Services Director
fbrantner@bdo.com

JAMES ROMAN
Cybersecurity, Compliance, and Assessments Services Senior Manager
james.roman@bdo.com

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.