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

Organizational Impact

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

The PCI Security Standards Council (PCI SSC) published V4.0 of the PCI Data Security Standards (PCI DSS) on March 31, 2022. With the transition period to adopt the new standards set to end on March 31, 2024, the outgoing version 3.2.1 will be retired, and V4.0 will become mandatory.

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

CHANGES TO THE PCI DSS REQUIREMENTS THAT ORGANIZATIONS SHOULD START PREPARING FOR NOW

As the transition period comes to an end, minor changes in the new version of the standards will need to be implemented when an organization is being assessed against V4.0. Major changes in V4.0 are a best practice until they become mandatory after March 31, 2025.

It's important to note that some of these major changes will require additional technology, resources, and time to successfully implement. We recommend working with your QSA to develop an implementation plan sooner rather than later.

The following are the changes that could have a large impact on an organization:

Multifactor Authentication (MFA)

Multifactor authentication was a requirement in PCI DSS version 3.2.1, primarily requiring MFA for access to the CDE, non-console administrative access to the CDE, and remote access including the CDE. In V4.0, the PCI SSC made clarifications to these requirements to assist organizations with understanding the intent for implementing MFA.

The most notable change to MFA is the introduction of the new future-dated PCI requirement 8.4.2. With this change, organizations are required to use MFA for all access to the CDE. This means all users accessing the CDE must be validated with MFA before they are granted access. This includes both users and administrators.

The important thing to note is that the requirement to use MFA for access to the CDE and the requirement to use MFA for non-console administrative access are separate requirements, and both controls must be in place for PCI compliance. For example, if an administrator is accessing a server in the CDE, the administrator must use MFA to access the CDE, and then use MFA a second time to authenticate access for non-console administrator activities.

When reviewing the MFA requirements, the QSA team will need to assess how the organization processes, stores, or transmits cardholder data. It will also be necessary to assess the systems that are connected to or that could impact the CDE. How the organization's network is configured will be another determining factor.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

Vulnerability Scans

There are also changes with regard to vulnerability scanning that organizations need to be aware of and should start planning for. Organizations will need to perform internal vulnerability scans via authenticated scanning. An authenticated scan can produce a more comprehensive output since the scanning tool has access to the entire system.

In addition to authenticated scans, organizations will be required to risk rank vulnerabilities that are not ranked as a high or critical risk. All other applicable vulnerabilities (lows and mediums) will need to be risked ranked and defined within the organization's targeted risk analysis.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

Protect Sensitive Authentication Data

Requirement 3 of the PCI DSS has numerous changes that will impact organizations that store cardholder data and sensitive authentication data (SAD). The protection of pre-authorized SAD was not a requirement in version 3.2.1, but it is in V4.0. Another part of the standards in version 3.2.1 is that an organization was not to retain SAD after authorization, unless an organization is able to demonstrate the business requirements for retaining the SAD and, in some instances, has received approval to retain SAD.

In V4.0, SAD that is stored electronically prior to completion of the authorization is required to be encrypted using strong cryptography. This could involve re-engineering processes and systems, including code development, and could take some time to implement. Storage of SAD after authorization requires the organization to follow the PCI requirements regarding the protection of stored data.

Note: This requirement is not eligible for the customized approach.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

Prevent Copy and/or Relocation of Primary Account Numbers (PAN)

PCI requirement 12.3.10 in version 3.2.1 is an administrative requirement to prevent remote access users from copying, moving, and storing cardholder data on to local hard drives and removable electronic media, unless explicitly authorized.

PCI requirement 3.4.2 in V4.0 includes the administrative requirement; however, the standard adds a technical control to prevent the copying or relocation of PAN when using remote access technologies. The remote access technology will need to be assessed to determine how the application is configured to prevent PAN from being copied or moved.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

Disk Encryption

If disk-level or partition-level encryption is used to render PAN unreadable, it is implemented only as follows:

- On removable electronic media.
- If used for non-removable media, PAN must also be rendered unreadable via another mechanism that meets requirement 3.5.1.

Disk-level encryption on computers, laptops, servers, and storage arrays is not appropriate to protect stored PAN if the data is decrypted upon user authentication. Disk-level and partition-level encryption typically encrypts the entire disk or partitions and decrypts the data automatically when a user or administrator authenticates to the system. For this reason, an alternative method for encrypting the data must be used. This effectively prevents disk encryption from being the only process to protect the PAN.

Effective examples would be file-level or column-level encryption.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

Customization Approach

The traditional process for securing and managing an organization's cardholder data environment was by complying with the PCI Council's Data Security Standards (DSS). The process uses a "Defined Approach" method where the requirements, testing procedures, and reporting instructions are well defined for each requirement.

V4.0 of the DSS is implementing a new approach referred to as a "Customized Approach." If an organization's processes do not align with the defined approach, but they are meeting the intent of the requirement, an organization may use the customized approach method to assess a particular requirement.

Documenting the customized approach is the organization's responsibility and should be completed before its PCI assessment commences. Please note: The customized approach will take extra effort for the organization and the assessor.

The organization must be able to demonstrate the following:

- The controls are in place to meet the intent of the original, defined approach requirement.
- The controls must meet the customized approach objectives.
- The customized approach implemented has been completely documented.
- Evidence exists and is maintained for each customized control.
- A targeted risk analysis has been completed.
- Testing and monitoring of the control occurs.

The assessor's role is to review the customized approach with the organization and agree to the approach. The process will include the review of the organization's evidence, understanding the testing procedure, and performing an independent test of the control(s).

Targeted Risk Analysis (TRA)

A TRA is defined as a risk analysis that focuses on a specific PCI DSS requirement(s) of interest, either because the requirement allows flexibility (for example, as to frequency) or, for the Customized Approach, to explain how the entity assessed the risk and determined the customized control meets the objective of a PCI DSS requirement.

Requirement 12.2 in version 3.2.1 of the PCI Data Security Standards (PCI DSS) requires organizations to implement a risk assessment at least annually that identifies critical assets, threats and vulnerabilities, and results in a formal, documented analysis of risk.

V4.0 of the PCI DSS removed requirement 12.2 and replaced this requirement with a new requirement: 12.3.1. The new requirement is to perform a TRA for any PCI DSS requirement that provides flexibility for how frequently it is performed, resulting in a TRA to be performed for the following requirements: 5.2.3.1, 5.3.2.1, 7.2.5.1, 8.6.3, 9.5.1.2.1, 10.4.2.1, 11.3.1.1, 11.6.1, 12.3.1, 12.3.2, and 12.10.4.1.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

Certificate Inventories

Expired and revoked certificates cannot be used. For this reason, PCI V4.0 has added new requirements requiring the organization to inventory its certificates and trusted keys that are implemented so all have been identified and documented. The entity must do the work to confirm that the certificates and keys are appropriately validated.

This activity should be performed as soon as possible, as it may take some time to collate certificate details for each algorithm in use and determine key expiry dates.

As part of the inventory process, an organization should keep track of the algorithms, protocols, key strength, key custodians, and key expiry dates. For certificates, the inventory should include the issuing CA and certification expiration date.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

Anti-phishing Mechanisms

Organizations need to implement a technical mechanism that is automated to protect users from phishing attacks. The automated mechanism will be brought into scope for PCI DSS; however, just the mechanism is in scope. For example, an automated process/ mechanism established within an email server would mean applicable PCI requirements would only apply to the process/ mechanism, not the entire email server.

Mechanisms that can detect and prevent phishing are often included in anti-malware solutions, and anti-malware is in-scope for PCI (see PCI requirement 5).

Note: The requirement to use anti-phishing mechanism may need to be extended to include other end-user messaging technologies. The anti-phishing mechanism needs to be an automated mechanism and cannot be met exclusively through security awareness training.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

Automated Detection and Alerting of Web-Based Attacks

Requirement 6.4.1 of V4.0 is the same as requirement 6.6 in version 3.2.1, initially. The requirement indicates that an organization can review its public web applications security using a manual method or an automated method. As of March 31, 2025, requirement 6.4.2 supersedes requirement 6.4.1 and requires an automated process. One approach to meet the requirement is to implement a web application firewall (WAF) to prevent malicious attacks in real time.

A WAF can be either on-prem or cloud-based and installed in front of public-facing web applications to check all traffic to detect and prevent web-based attacks. The WAF should be configured to detect and generate alerts so that vulnerabilities can be mitigated.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

Protection of the Payment Page

Requirement 6.4.3 is a new requirement and focuses on unauthorized code. The requirement and controls are intended to reduce the likelihood of unauthorized code from running in the payment page when rendered from the cardholder's browser. All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:

- A method is implemented to confirm that each script is authorized.
- A method is implemented to assure the integrity of each script.
- An inventory of all scripts is maintained with written justification as to why each is necessary.

Using techniques to validate the integrity of the scripts executed on the client's browser to prevent tampering with the scripts will minimize the probability of unauthorized behavior, such as skimming the cardholder data from the payment page.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

Change and Tamper Detection — HTTP Header

In addition to requirement 6.4.3 above, there is an additional requirement (11.6.1) that discusses the implementation of a mechanism to evaluate the HTTP header and payment page. The mechanism must have change and tamper detection that runs at least once a week or periodically based on the organization's TRA. The mechanism must be able to alert personnel if unauthorized modifications are made to the HTTP header or payment page.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

Automated Log Reviews

Due to the amount of log data that is generated, there is a new requirement for the use of automated mechanisms to perform audit log reviews. Log harvesting, centralized log servers, and alerting tools, as in a security information and event management (SIEM) solutions, can help facilitate the process.

This requirement is a best practice until March 31, 2025, when it becomes mandatory.

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