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

Software Development Requirement Changes

SOFTWARE DEVELOPMENT REQUIREMENT CHANGES

V4.0 of the Payment Card Industry Data Security Standards (PCI DSS) software development requirements have been updated to protect applications that store, process, or transmit cardholder data, including web-based payment pages. The requirements are as follows:

- **6.1** Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.
- **6.2** Bespoke and custom software are developed securely.
- **6.3** Security vulnerabilities are identified and addressed.
- **6.4** Public-facing web applications are protected against attacks.
- **6.5** Changes to all system components are managed securely.

The changes to Requirement 6 in the PCI V4.0 standard are a best practice until the requirements become mandatory after March 31, 2025. When the future-dated requirements become mandatory, requirement 6.4.1 will be superseded by requirement 6.4.2. This new requirement makes it mandatory that an automated technical solution is deployed to detect and prevent web-based attacks.

6.4.2 For public-facing web applications, an automated technical solution is deployed that continuously detects and prevents web-based attacks, with at least the following:

- Installed in front of public-facing web applications and configured to detect and prevent web-based attacks
- Actively running and up to date as applicable
- Generating audit logs
- Configured to either block web-based attacks or generate an alert that is immediately investigated

The recommendation for this requirement includes using a web application firewall (WAF).

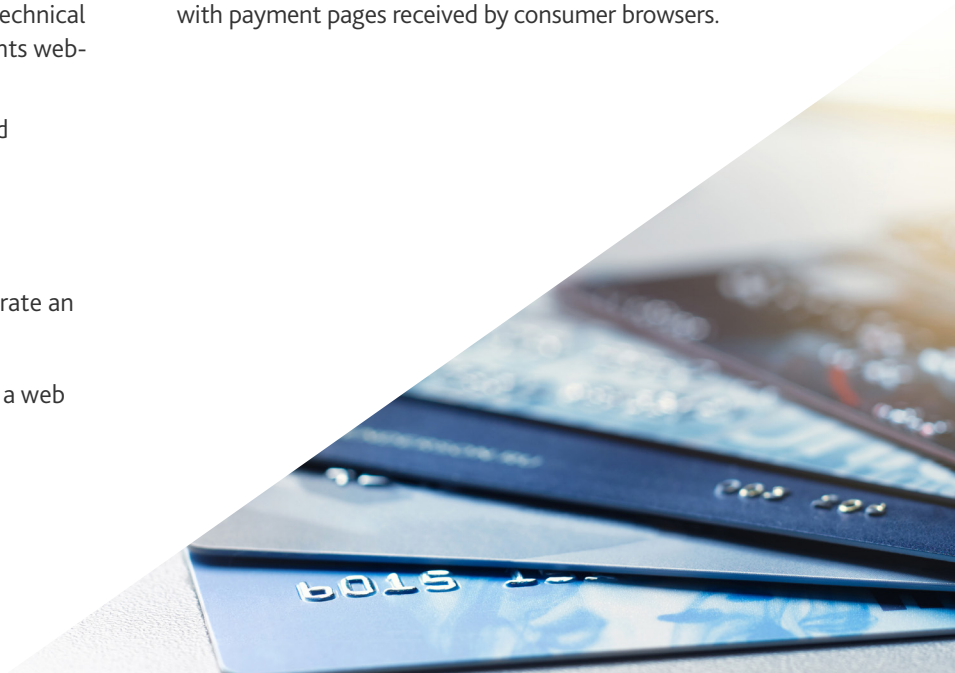
Another mandatory requirement going into effect on March 31, 2025, is Requirement 6.4.3: All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:

- 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

This requirement applies to all scripts, including scripts loaded from the entity's environment or from third and fourth parties.

Guidance for this requirement includes implementing one of several different mechanisms including but not limited to sub-resource integrity (SRI), content security policies (CSP), or a tag-management system.

A related, new requirement is found in Requirement 11 and makes it mandatory to deploy change- and tamper-detection mechanisms to verify that skimming code or similar techniques cannot interfere with payment pages received by consumer browsers.



11.6.1 A change- and tamper-detection mechanism is deployed as follows:

- To alert personnel to unauthorized modifications (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.
- The mechanism is configured to evaluate the received HTTP header and payment page.
- The mechanism functions are performed as follows:
  - At least once every seven days **OR**
  - Periodically (at the frequency defined in the entity's targeted risk analysis (TRA), which is performed according to elements specified in Requirement 12.3.1)

This requirement is intended to ensure changes to the assembled web objects that may perform malicious activity are detected on the consumer's browser and alert personnel to the unauthorized modification.

This requirement can be implemented via CSP, synthetic user monitoring, tamper-detection scripts, or reverse proxies and content delivery networks.

Requirements 6.4.2, 6.4.3 and 11.6.1 are considered to be best practices until March 31, 2025, when they become mandatory.

APPLICABILITY OF NEW REQUIREMENTS

Requirements 6.4.2 and 6.4.3 apply to bespoke and custom applications. The PCI Security Council uses the following definitions to clarify the applicability of these requirements:

- Bespoke software is developed for the entity by a third party on the entity's behalf and per the entity's specifications.
- Custom software is developed by the entity for its own use.

Entities must keep an inventory of all bespoke and custom software and include API development libraries.

Most notable is requirement 11.6.1. This requirement is applicable to all web-based payment applications, including those using third-party payment pages through an iFrame element or web redirection. In these instances, requirement 11.6.1 applies to the pages hosted by the entity that provide the address (URL) of the merchant's payment page.

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.

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