## Information Security

### PCI DSS 4.0

The Payment Card Industry Security Standards Council (PCI SSC) recently released a new version of the Payment Card Industry Data Security Standards (PCI DSS 4.0). This release contains some significant changes/enhancements to the standard, as well changes to the way that merchants and service providers are validated to the standard. Given the breadth of these changes, the PCI SSC has expanded the phase-in period for both migration to the new standard and some of the requirements contained within the standard.

Timeline

Description automatically generated

The following is the new standard available for download from the council’s website (<https://www.pcisecuritystandards.org/>). I highly recommend that your organization immediately review it for impact on your organization, as some of the enhancements that are being required may take significant time and resource to implement.

There are a few major structural considerations for PCI DSS v4.0:

* **Customized Approach:** First and foremost is the implementation of the concept of a “Customized Approach.” Effectively this is the PCI Security Standards Council’s (SSC’s) recognition of the appositeness for a more risk-based approach to PCI. Functionally, this means almost every requirement in v4.0 can be addressed by either meeting the explicit requirement in the “Defined Approach,” with a compensating control, or the intent of the requirement can be achieved through an entity’s own control definition based on “Customized Approach Objectives.”
* **Numbering Scheme:** The numbering scheme of the requirements in v4.0 have almost all changed. There is potential impact with your internal Governance Risk and Compliance (GRC) systems where you may be tracking evidence across your organization for multiple different compliance frameworks within your organization.
* **Clarifying Intent:** The SSC did a commendable job of clarifying the intent of some of the more ambiguous requirements. For example, previous versions of the Data Security Standard (DSS) requirement 2 (“*Do not use vendor-supplied defaults for system passwords and other security parameters*”) intermingled general and wireless network specific considerations. DSS 4.0 requirement 2 (“*Apply Secure Configurations to All System Components*”) has consolidated all the wireless security controls into requirement 2.3.
* **Significant Reporting Template Changes:** There are two significant changes in the way Qualified Security Assessors (QSAs) are required to report an entity’s compliance on both the Report on Compliance (ROC) and the client-facing Attestation of Compliance (AOC).
* **New Compliance Status:** The AOC now indicates whether a **Full Assessment** or a **Partial Assessment** was performed. This enables an organization to perform an assessment on specific environments or controls and receive an AOC that is specific to the scope of the assessment (e.g., only physical security, cloud environment, secure software development, etc.).
* **In Place with Remediation:** The QSA is required to use this status when the following is true:

*The requirement was Not in Place at some point during the PCI DSS assessment period of the entity, but where the entity remediated the issue such that the requirement was In Place before completion of the assessment. In all cases of In Place with Remediation, the assessor must have assurance that the entity has identified and addressed the reason that the control failed, has implemented the control, and has implemented ongoing processes to prevent re-occurrence of the control failure.*

Could there be legal implications to a Service Provider who provides a copy of its Attestation of Compliance when there are “In Place with Remediation” statuses?

#### Key New Requirements

PCI DSS v4.0 brings a total of sixty-one new requirements to the Standard, which admittedly seems like a large amount. Breaking it down further, fifty-one of the new requirements apply to all entities, while ten of them only apply to Service Providers. Furthermore, many of these new requirements are sub-requirements expanding on previously established principals. Finally, twelve of the new sub-requirements are the same for each of the twelve top-level requirements, requiring a formal definition of the roles and responsibilities for performing activities in each top-level requirement (much like DSS v3.1 included 12 new requirements for general policies and procedures for each top-level requirement).

Looking at the new requirements from a CISO perspective, these are a few of the most notable new requirements you will probably hear most angst about in your hallways:

* + There are two significant and potentially impactful changes to Multi-Factor Authentication requirements:
* MFA systems must be hardened to prevent bypass (even for administrators for troubleshooting). This means alternative methods of access (e.g., backup-admins, on premise, or remote machine console) should be maintained to prevent extended downtimes should very bad things happen!
* All access into the Cardholder Data Environment (CDE) must use MFA; this may require your teams to use MFA twice—one for remote access, and then again for access into the CDE.
* There is a modest, but substantial change to Requirement 10 if you aren’t using an automated solution for daily log reviews. Entities are now required to use automated mechanisms for performing daily log reviews. This could cause a hit to your budget, but luckily this isn’t applicable until March 31, 2025.
* There are several significant changes for Requirement 11:
* **Timing for Vulnerability Scans:** Vulnerability scans, external and internal, must be performed every 90–91 days, or on the same day every third month, and after significant changes. This used to state quarterly, but the Council is cracking down on these being performed in a more regular cadence.
* **Authenticated Scans:** Internal vulnerability scans now must be authenticated scans. This may cause some work on the part of your team to have clean authenticated internal scans.
* **Vulnerability Scanning Remediation:** The new Standard now requires “all other vulnerabilities,” (e.g., medium and low) to be corrected and re-scanned within a timeline determined through a targeted risk assessment. Let’s repeat: all vulnerabilities must be fixed at some specified point.
* **Overt Malware Communication Channels:** Service Providers must now use intrusion detection or prevention systems to detect, alert on, or block covert malware communication channels, such Cylance, or another next gen endpoint protection application.
* **Payment Page Tamper Detection:** There is now a requirement to include client-side change and tamper detection for payment pages. The goal is to ensure, as best you can, that the payment page the consumers get is the payment page you expect them to get, and nothing else.
* One of the largest changes in PCI DSS v4.0 is mandated use of targeted risk assessments for the following:
  + All uses of the Customized Approach must include a targeted risk assessment.
  + Each PCI requirement that provides flexibility for how frequently it is performed must be supported by a targeted risk assessment.
* There is now a requirement to review hardware and software technologies at least once every 12 months to ensure the technologies accomplish the following:
  + continue to receive security fixes from vendors promptly;
  + continue to support (and do not preclude) the entity’s PCI DSS compliance;
  + document industry announcements or trends such as announced “end of life” plans; and
  + document a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced “end of life” plans.

### Strengthening American Cyber Security Act

On March 15, 2022, the Strengthening American Cybersecurity Act, which includes the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the Act) was signed into law by President Biden, thereby creating new reporting requirements for critical infrastructure entities. Under the Act, once implementing regulations are issued (which are not expected this year—*see below on when the reporting requirements will occur*), covered entities will be subject to two new reporting requirements:

1. Covered entities must report covered cyber incidents no later than 72 hours after the covered entity reasonably believes that an incident has occurred.
2. Covered entities that make ransom payments because of a ransomware attack against critical infrastructure must report the payment no later than 24 hours after payment has been made.

Although the Act has been signed into law, the Director of CISA has up to 24 months to publish a notice of proposed rulemaking. The Act also permits an additional 18 months after the notice for an issuance of a final rule. This timeline is important to keep in mind, as much of the Act instructs the Director of CISA to establish clear reporting guidelines and regulations. Before the Director issues a final rule, key definitions such as what constitutes a "covered cyber incident" and what entities qualify as "critical infrastructure" remain unclear.

Critical infrastructure includes the assets, systems, facilities, networks, and other elements that society relies upon to maintain national security, economic vitality, and public health and safety. The Current U.S. Critical Infrastructure Sectors are as follows:

|  |  |  |
| --- | --- | --- |
| * Chemical | * Commercial Facilities | * Financial Services |
| * Food and Agriculture | * Communications | * Government Facilities |
| * Critical Manufacturing | * Dams | * Transportation Systems |
| * Nuclear Reactors | * Information Technology | * Defense Industrial Base |
| * Energy | * Materials, and Waste | * Emergency Services |
| * Healthcare and Public Health | * Water and Wastewater Systems |  |

## US Privacy

### Transatlantic Data Privacy Framework

In July of 2020, the European Court of Justice (ECJ) ruled that the Privacy Shield program that provided safe harbor for data transfers from the E.U. and Switzerland to the US did not provide adequate privacy protections for E.U. citizens, thus revoking the safe harbor associated with participation in the program. After two years of limbo there has finally been some movement regarding the Privacy Shield issue. The E.U. and U.S. have agreed in principle to the “Transatlantic Data Privacy Framework” which will go into effect after President Biden signs an Executive Order (EO) that addresses the scope and proportionality of permissible U.S. national security surveillance activities and creates redress mechanisms for Europeans whose personal data is determined to have been collected improperly by U.S. intelligence agencies. Once the EO is in place, the ECJ believes adequate protections for E.U. citizens (Adequacy) will have been achieved and U.S. companies can again rely on the U.S. Commerce Department’s Privacy Shield program for safe harbor.