protiviti®
Global Business Consulting

PCI Security Standards Council publishes updated data security standard

DSS 4.0 addresses rapidly evolving threat environment and provides flexibility for how organisations can achieve compliance

On March 31, 2022, the PCI Security Standards Council (PCI SSC) released a new version of the PCI Data Security Standard (DSS). PCI DSS 4.0 is the first revision to the DSS in almost four years. It represents a major update to the standard as the payments industry faces an evolving threatscape.

Rapidly expanding adoption of cloud and other emerging technologies made it necessary to update the PCI DSS standard to reflect the current environment, respond to new threats with evolution of requirements, and provide additional guidance for compliance validation.

PCI DSS 4.0 and the related Summary of Changes will be translated into several languages and published over the next several months to support global adoption of the new standard.

Changes to the standard

The updates in PCI DSS 4.0 address emerging threats and technologies while continuing to meet the security needs of the payments industry. The revised standard adds flexibility to support innovation and allows organisations to adopt their own methodologies for meeting compliance objectives.

Other revisions in version 4.0 include:

- Structural changes to the standard itself, including removing some redundant testing procedures, renumbering requirements, and combining requirements that support the same intent while separating requirements that support different intents
- Adding more guidance in the introduction and to individual requirements
- Clarifying ambiguous requirements and testing procedures identified by the payment information security community

Customised vs. Defined Approach methods

One of the most significant changes in PCI DSS 4.0 is a newly created alternative method for PCI compliance validation called the Customised Approach. In this method, the PCI DSS defines only the

objective of the requirement and allows for flexibility in meeting the objective in the way best suited for the entity. The entity must design the control, conduct risk assessments, implement the control and test its effectiveness. The use of the Customised Approach will require more formal documentation than has typically supported testing in the past, as all of these steps will need to be documented in accordance with requirements outlined in PCI DSS 4.0 and reviewed by a Qualified Security Assessor (QSA) during the compliance validation process. In addition to confirming that the control designed through the Customised Approach meets the objective, the QSA must independently derive an appropriate testing procedure and test the control to confirm it is functioning properly.

The Defined Approach, in contrast, follows the traditional validation process in which control and testing procedures are defined and must be followed. This aligns with the familiar method of testing that has existed for many years in various versions of the PCI DSS. The Defined Approach is best suited for organisations with defined controls in place and a desire for more structure and guidance. As opposed to the Customised Approach, the Defined Approach still allows for the use of compensating controls just as they were used under previous versions of the PCI DSS.

Organisations can combine the Defined and Customised Approaches within the same assessment on a per-requirement basis or can leverage different approaches for different components of the environment. Entities validating PCI DSS compliance via self-assessment are not eligible for the Customised Approach.

Other notable changes and requirements

The PCI DSS 4.0 is much more precise and provides a clear definition of time frames for time-bound controls. Any controls required to be performed "periodically" must be formally defined and supported by a documented risk analysis to justify the period in which the entity determines the control is performed. Additionally, each of the 12 PCI DSS requirements now mandates assigning roles and responsibilities for all activities in each respective requirement.

Below are some additional new requirements that may require extra planning and potential implementation of new solutions and/or processes if they are not already in place. Organisations should consult the published PCI DSS 4.0 for the full list of changes in the standard.

- PCI DSS 4.0 requires the entity to perform a formal PCI compliance scope confirmation. This confirmation must be documented at the level of detail prescribed by the respective PCI DSS requirement (Requirement 12.5.2).
- A technical control will now have to be implemented to prevent copy and/or relocation of card number information for personnel connecting remotely, except for those with documented authorisation and a legitimate, defined business need (Requirement 3.4.2). Under PCI 3.2.1 this was a policy-only requirement that did not call for a technical control.
- Disk-level encryption as the only method for encrypting cardholder data will now be acceptable only for removable media. Cardholder data stored on non-removable media will have to be additionally encrypted by other means meeting PCI DSS requirements (Requirement 3.5.1.2).
- Phishing and social engineering attacks are one of the primary attack vectors leveraged by attackers for successful breaches. PCI DSS 4.0 calls for technical controls to detect and protect against phishing

attacks (Requirement 5.4.1) and requires organisations to include education about phishing and social engineering threats in their security awareness training (Requirement 12.6.3.1).

- A web application firewall (WAF) is now required to protect all internet-facing web applications (Requirement 6.4.2). The previous version of PCI DSS provided an alternative to WAF by leveraging review of public-facing web applications via manual or automated application vulnerability security assessment tools.

Enhanced access control requirements

While previous versions of the PCI DSS did not mention system and application accounts, several new requirements for formalised management of system and application accounts are included in PCI DSS 4.0 (Requirement 7.2.5), along with periodic review of (Requirement 7.2.5.1) and password protection for (Requirement 8.6.1) those accounts. Organisations must ensure that application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code (Requirement 8.6.2). Static code analysis tools can help discover hard-coded passwords in code. Alternatively, a data loss prevention (DLP) tool could be used to search for credentials in scripts or config files.

User accounts will need to be reviewed every six months to ensure that the user is legitimate and is being granted appropriate access, and these reviews will need to be documented (Requirement 7.2.4). Organisations subject to Sarbanes-Oxley (SOX) compliance may be able to leverage or build on existing quarterly account review procedures established for SOX. The same process must be applied to system/application accounts, however these accounts could be reviewed "periodically," with frequency defined via documented risk analysis.

The requirement for the use of multifactor authentication (MFA) has been expanded to require all access to the cardholder data environment to require MFA (Requirement 8.4.2). Additionally, PCI DSS 4.0 clarifies that MFA must not be susceptible to replay attacks like a one-time password-based MFA, and must be implemented in a way so it cannot be bypassed by any users, including administrators, unless specifically authorised for a limited time (Requirement 8.5.1). The new requirement also requires success of all authentication factors to be validated before access is granted. At the same time, MFA is not required for access to in-scope system components that are not in the cardholder data environment (CDE).

Enhancements to requirements for monitoring

Organisations that need to comply with PCI DSS are now required to implement Security Information and Event Management (SIEM) solutions (Requirement 10.4.1.1). SIEM solutions are an effective way to monitor security events and identify potential security incidents and are a common practice in the industry.

PCI DSS 4.0 expands the requirement to monitor for failures in critical security controls like firewalls, intruder detection systems (IDS)/intruder prevention systems (IPS), change-detection solutions, anti-malware tools, logical access controls and physical access controls to apply to all entities rather than only to service providers. Monitoring and addressing failures of SIEM and security testing tools has been

added to the scope of the requirement (Requirement 10.7.2). An additional requirement defining required components of response to failure of critical security controls also is now applicable to all entities and not just service providers (Requirement 10.7.3).

Increased security for payment pages

To drive security for payment pages, PCI DSS 4.0 introduces two new requirements. Any scripts loaded in the payment page must be inventoried, explicitly authorised and have a method in place to ensure integrity of each script in payment pages (Requirement 6.4.3). It is important to note that the scope of this requirement is the payment page itself, not the rest of the website. The requirement applies to any scripts loaded within the payment page, including those provided by third parties like advertising or chatbots. If scripts on a payment page are necessary, Subresource Integrity (SRI) or Content Security Policy (CSP) could be leveraged to meet the requirement.

Another new requirement calls for implementing a change-detection or tamper-detection mechanism to alert the organisation to unauthorised modification to the HTTP headers and the contents of payment pages as received by the consumer browser. The control must evaluate the received HTTP header and payment page at least weekly or at a frequency supported via documented risk analysis conducted by the entity (Requirement 11.6.1). To meet this requirement, organisations could leverage synthetic monitoring tools that simulate user interaction with the web application. Alternatively, violations of the CSP or changes to the CSP could be used to detect suspected tampering.

Upgrades to legacy systems

The security challenges posed by vulnerabilities on legacy or "end of life" systems are well known to security professionals. PCI DSS 4.0 introduced a new requirement to review hardware and software technologies in use for availability of support and security fixes, as well as announcements of "end of life" or retirement of the technology by respective vendors. The requirement also calls for a documented remediation plan for outdated technologies to be approved by senior management (Requirement 12.3.4). To achieve compliance, organisations will need to budget and plan for timely upgrades. Extended support, if available, may be one option to meet the requirement.

Maintaining compliance

Another important requirement introduced in PCI DSS 4.0 is to conduct a review every three months to confirm personnel are performing their tasks in accordance with all security policies and all operational procedures. The requirement mandates reviews be performed by personnel other than those responsible for performing the given task, and for results of the reviews to be documented along with remediation actions taken for any tasks that were found to not be performed (Requirement 12.4.2). The results of the reviews must be signed off by the personnel assigned responsibility for the PCI DSS compliance programme (Requirement 12.4.2.1). The organisation's Internal Audit team would be in the best position to conduct such reviews, as Internal Audit is inherently independent of the departments responsible for maintaining PCI compliance and understands the requirement for documentation and supporting evidence. Compliance with this requirement could make an annual assessment by a QSA more predictable, with fewer instances of noncompliance.

The transition clock is ticking

Recognising the significant number of changes introduced in the new PCI DSS standard, PCI SSC established a transition timeline from version 3.2.1 to version 4.0. Under this timeline, PCI DSS 3.2.1 will remain active for two years, and will be retired on 3/31/2024. Starting on that date, all new assessments will need to use PCI DSS 4.0 to validate PCI compliance. Additionally, most of the new requirements will be considered best practices until 3/31/2025, at which point they will become mandatory. The only new requirements that will be mandatory on 3/31/2024 are those requirements for assigning and documenting roles and responsibilities for activities in each section, the requirement for performing targeted risk analysis for each requirement met with the Customised Approach, and the requirement to document and confirm the scope of PCI compliance annually.

Within a few months, PCI SSC will release Self-Assessment Questionnaires (SAQ) for PCI DSS 4.0, as well as an updated version of the Prioritised Approach document. We will continue to keep you informed about the new updates and additional guidance released for this new standard.

What companies should do to prepare

While there are still almost three years until most of the new requirements in PCI DSS 4.0 require mandatory compliance, organisations should begin preparations by conducting a gap assessment against the new requirements as soon as possible, given the number of new requirements and resource demands for implementation of the updated standard. Once compliance gaps are identified, a remediation plan must be developed to ensure gaps are addressed by the time the new requirements go into effect and controls have been able to demonstrate effective operation for a period of time.

In planning remediation, organisations should not only consider scope reduction opportunities, but also should examine potential benefits of the Customised Approach introduced in PCI DSS 4.0 for their organisation. Additionally, existing projects and initiatives planned by entities should be evaluated in light of the newly released PCI DSS standard. Some projects may require adjustments to scope to address the requirements, while others may need to be reprioritised to ensure compliance requirements are achieved by the established deadline.

Staffing and training levels should be analysed to ensure adequate capabilities are in place for the newly required processes. For example, the process of semiannual review of user accounts and periodic review of system and application accounts may require additional resources. The requirement to conduct formalised reviews every three months to confirm tasks required by PCI DSS are performed as intended will not only require identified resources to perform these reviews but will also need to ensure personnel tasked with these reviews are qualified and trained to conduct such assessments. While the Internal Audit department would be the best fit to be responsible for these reviews from an independence perspective, some Internal Audit teams will have to be upskilled to conduct internal PCI reviews.

Given how pervasive legacy (“end-of-life”) systems may be in organisations, the requirement to remediate outdated technologies could require a multifaceted approach for companies, involving not just resource-intensive upgrades, but also process changes, outsourcing, and potentially compensating controls for instances when core business applications relying on legacy technologies cannot be upgraded in a timely manner.

How Protiviti can help

Protiviti has been involved with PCI since inception of the Data Security Standard in 2002, before the PCI Security Standards Council was formed. As one of the largest and most experienced QSA firms, we have completed numerous PCI compliance assessments for clients ranging from upper midsized organisations to Fortune 500 companies across many industries.

Protiviti is a PCI SSC approved global provider for the following programmes:

- Qualified Security Assessors (QSA)
- Payment Application QSAs (PA-QSA)
- Qualified PIN Assessor (QPA)

Our global PCI Planning, Readiness and Compliance professionals will work with your organisation to conduct a PCI 4.0 compliance gap assessment to understand what requirements are not currently in place and require remediation. We can then advise you on the most effective and efficient methods for achieving compliance, whether it involves implementing a new solution, changing or outsourcing a process, implementing compensating controls, or planning for a Customised Approach to some of the requirements.

We can also provide:

- Annual on-site audits
- Quarterly vulnerability scans
- Annual penetration testing
- Programme Governance & Technical Remediation
- Visa PIN Security reviews

Contacts

Chip Wolford
+1.513.362.1716
chip.wolford@protiviti.com

Daniel Baron
+1.213.327.1502
daneil.baron@protiviti.com