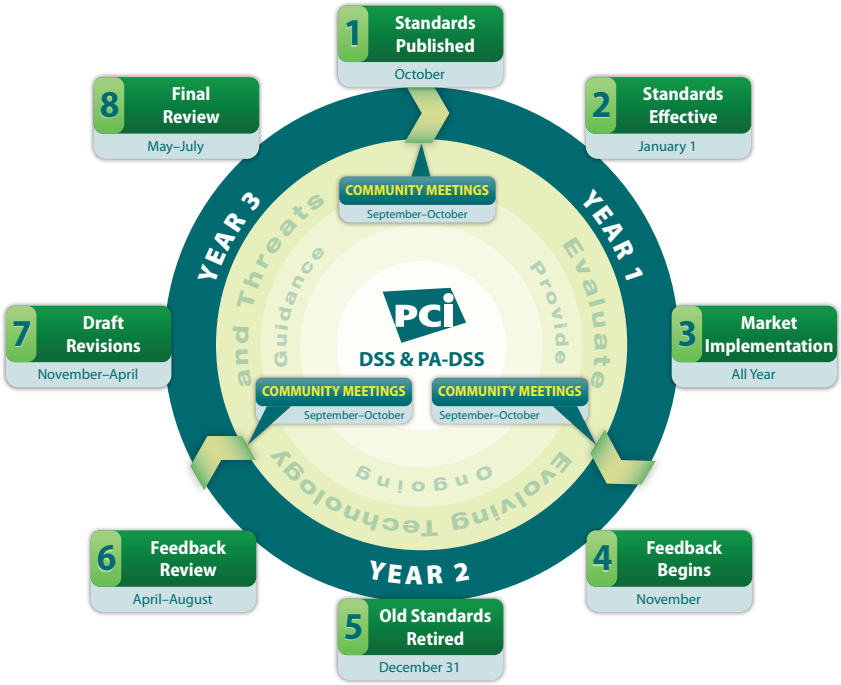
Lifecycle for Changes to PCI DSS and PA-DSS

The Payment Card Industry Data Security Standard (PCI DSS) secures cardholder data that is stored, processed or transmitted by merchants and other organizations. The standard is managed by the PCI Security Standards Council (PCI SSC). Input for proposed changes to the standard is also made by PCI SSC stakeholders – Participating Organizations, including merchants, banks, processors, hardware and software developers, Board of Advisors, point-of-sale vendors, and the assessment (QSA & ASV) community.



Changes to the PCI standards follow a defined 36-month lifecycle with eight stages, described below. The lifecycle ensures a gradual, phased introduction of new versions of the standard in order to prevent organizations from becoming noncompliant when changes are published. This lifecycle also applies to the Payment Application Data Security Standard (PA-DSS), which covers validation requirements for applications used to process payment cards. During the lifecycle, the Council will continuously evaluate evolving technology and threats, and if necessary, make mid-lifecycle changes to the standards or provide ongoing supplemental guidance about these issues.

NEW STANDARDS PUBLISHED

- Major new releases of PCI DSS and PA-DSS
- Presented at Community Meetings in September & October
- Initiates 3-year lifecycle
- Previous versions remain effective for 14 months

Stage 1: Standards Published

Stage 1 occurs in October of Year 1 after the Council's annual Community Meetings and initiates a new lifecycle for the PCI DSS and the PA-DSS. Stakeholders may immediately implement the new standards, but are not required to do so until after they become effective.

Stage 2: Standards Effective

The second stage occurs on January 1 of Year 1. On this date, the new standards become effective. Stakeholders should begin using the new standards as the basis for their payment security programs as of this date. For purposes of validation for compliance, the old standards are grandfathered for 14 months. Nevertheless, the Council urges stakeholders to complete their transition to the new standards as quickly as possible, particularly where any new control requirements are critical for protecting cardholder data.

Stage 3: Market Implementation

During the third stage, the market completes its implementation of the new standards. This entails assessing changes to the new standards and determining their applicability to a stakeholder's cardholder data environment. Stage 3 occurs throughout Year 1, which provides for an orderly, phased implementation of any required changes.

NEW STANDARDS ERRATA

- Occasionally new standards may require minor changes or errata
- The Council may publish errata at any time if so required
- If errata are required, they usually will become effective immediately

Stage 4: Feedback Begins

The fourth stage initiates a period of systematic feedback from stakeholders on the new standards. Stakeholders will have the opportunity to formally express their views on the new standards and provide suggestions for changes and improvements – especially in light of evolving technology and threats to cardholder data. The Council will clearly communicate with all stakeholders the process of how to submit feedback during this stage. Systematic consideration and incorporation of stakeholder feedback is vital for drafting forthcoming versions of the standards. Stage 4 occurs during November to March of Year 2.

Stage 5: Old Standards Retired

Stage 5 occurs on December 31 of Year 2. On this date, the old PCI DSS and PA-DSS standards are retired. After this date, all validation efforts for compliance must follow the new standards.

COMMUNITY MEETINGS

- Occur during September and October each year
- Provide the Council opportunity to discuss standards with Participating Organizations
- Provide opportunity for Participating Organiza-tions to share feedback with the Council
- Ensure the Standards are meeting their objectives

Stage 6: Feedback Review

The sixth stage is for collecting and evaluating feedback from Participating Organizations. In processing the thousands of inputs, feedback is typically categorized as follows:

- Clarifications –requests about language in standards that may be perceived as confusing. The goal of addressing clarification feedback is to ensure that concise wording in the standards portray the desired intent of requirements.
- Additional Guidance –identifies a need for further detail in understanding the intent of a requirement. The goal of addressing additional guidance feedback is to provide further information on a particular topic typically via FAQs, Information Supplements, or the DSS Navigation Guide.
- Evolving Requirements – requests and feedback that outline a particular situation not addressed in a standard. The goal of addressing evolving requirements feedback is to ensure that the standards are up to date with emerging threats and changes in the market.

Stage 6 occurs during April through August of Year 2.

Stage 7: Draft Revisions

During stage 7 new standards are drafted based on research, analysis and stakeholder input. Drafts are prepared by the Council's Technical Working Group and disseminated within the Council for internal review. Stage 7 occurs during November through April of Year 3.

Stage 8: Final Review

Final draft review of the new standards and related supporting documents occurs during stage 8. Drafts are shared internally within the Council and with the Board of Advisors for review and comment. The Council also makes final adjustments to the drafts by incorporating feedback from this review. During this stage, the Council provides a "summary of changes" document to the stakeholder community with clear, precise guidance on what to expect in the new standards. The final versions of the new standards and supporting documentation are prepared for publication and release at the next Community Meetings. Stage 8 occurs during May through July of Year 3. A new three-year lifecycle begins upon publication of the new standards to the Council's website at www.pcisecuritystandards.org.