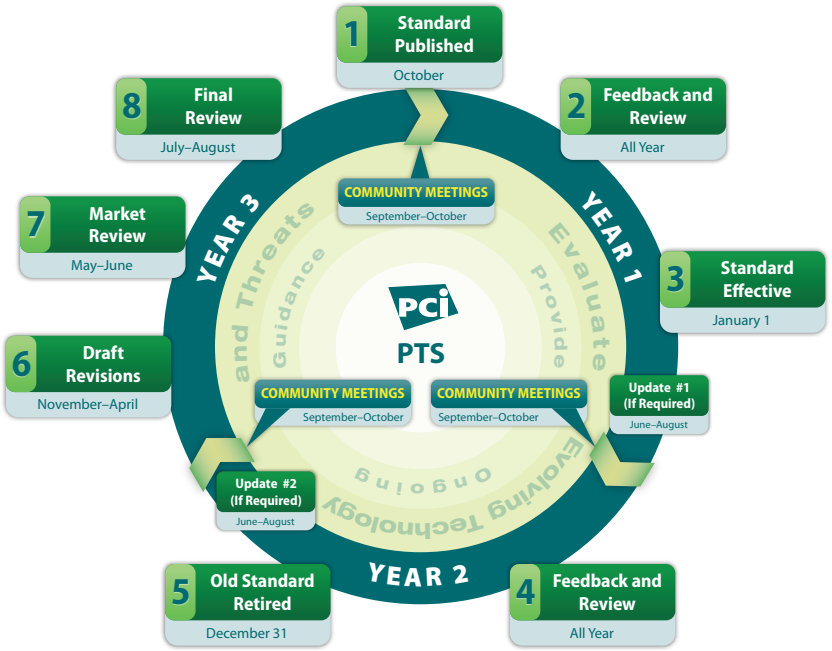
Lifecycle for Changes to PTS

The Payment Card Industry PIN Transaction Security (PTS) requirements are used primarily by ATM and point-of-sale equipment manufacturers to secure cardholder data at the physical point of interaction. The standard is managed by the PCI Security Standards Council (PCI SSC). Input for proposed changes to the standard are also made by PCI SSC stakeholders – Participating Organizations, including merchants, banks, processors, hardware and software developers, point-of-sale vendors, and approved security evaluation laboratories.



Changes to the standard follow a defined 36-month lifecycle with eight stages, described below. The lifecycle ensures a gradual, phased use of new versions of the standard without invalidating current implementations of PTS. It also prevents organizations from becoming noncompliant when changes are published and allows vendors to complete existing product development. Throughout the lifecycle, the Council will continuously evaluate evolving technology and threats, and provide ongoing guidance about these standards.

NEW STANDARD PUBLISHED

- Major new release of PTS
- Presented at Community Meetings in October
- Initiates 3-year lifecycle
- Previous version remains effective for 12 months after the new standard becomes effective

Stage 1: Standard Published

Stage 1 occurs in October of Year 1 with the publication of the new standard; this initiates a new lifecycle for PTS. The new standard contains updates for ensuring an optimal level of security to the terminal for protecting cardholder data.

Stage 2: Feedback & Review

Stage 2 is an ongoing process of feedback and review occurring throughout Year 1. Feedback is actively sought from all Participating Organizations, security evaluation laboratories, the PCI PTS Working Group, and the PCI Security Standards Council. The goal is assessing the effectiveness and applicability of the new standard. Feedback can enable guidance for interpreting the standard, and how evaluation laboratories should collectively use similar methodologies for testing identical solutions.

If a new threat represents a significant security risk, the PCI Security Standards Council will take immediate action to help stakeholders understand how to minimize the threat and protect cardholder data.

NEW STANDARD ERRATA

- Occasionally a new standard may require minor errata
- The Council may publish errata at any time if so required
- If errata are required, they usually will become effective immediately
- If required, more detailed Updates to PTS may be published prior to Community Meetings in Years 1 and 2

COMMUNITY MEETINGS

- Occur during September and October each year
- Provide the Council opportunity to discuss issues with participating organizations
- Provide opportunity for participating organizations to share feedback with the Council
- Ensure that PTS is meeting its objectives

Stage 3: Standard Effective

On January 1 of Year 1, the new standard becomes effective. Stakeholders should begin using the new standard as of this date. The old standard will remain effective for 12 months to facilitate vendors who are completing developments or have devices under PTS evaluation. The Council urges stakeholders to complete their transition to the new standard as quickly as possible, particularly where new control requirements are critical for protecting cardholder data.

Stage 4: Feedback & Review

The Stage 4 process of feedback and review continues throughout Year 2. The review process may result in minor updates to the standard. As during Year 1, additional guidance may be published on the Council website in updates to the PCI PTS Frequently Asked Questions, in supplemental white papers, or other supporting documents.

Stage 5: Old Standard Retired

Stage 5 occurs on December 31 of Year 2. On this date, the old PTS standard is retired. After this date, all new device security evaluations must be performed against the new standard.

Stage 6: Draft Revisions

The sixth stage of the lifecycle is for drafting a new PTS standard that clarifies or improves the current standard based on prior research, analysis, and input by stakeholders. Drafts are prepared by the Council's Technical Working Group and disseminated within the Council for internal processing and development. Stage 6 occurs during November through April of Year 3.

Stage 7: Market Review

The 60-day market review stage is a formal feedback process where the "redline draft" is shared for review and comment by key stakeholders. Market reviewers include Participating Organizations, PTS vendors/manufacturers, and the Council's Board of Advisors. Stage 7 occurs during May – June of Year 3.

Stage 8: Final Review

The last stage of the lifecycle is for final review of drafts of the new standard and related supporting documents. Drafts are shared internally within the Council and with the Board of Advisors for review and comment. The Council makes final adjustments to the drafts by incorporating feedback from this review. 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 July – August of Year 3. A new three-year lifecycle begins upon publication of the new standard at www.pcisecuritystandards.org.