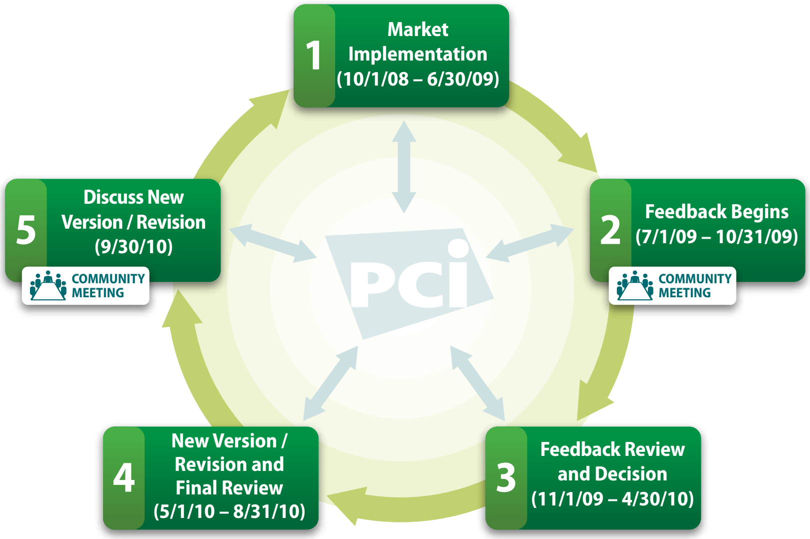
Lifecycle Process for Changes to PCI DSS

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) and its founders – American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Input for proposed changes to the standard is also made by PCI SSC stakeholders —participating organizations, including merchants, banks, processors, hardware and software developers, point-of-sale vendors and the assessment (QSA & ASV) community.


1 Market Implementation (10/1/08 – 6/30/09)
2 Feedback Begins (7/1/09 – 10/31/09)
COMMUNITY MEETING
3 Feedback Review and Decision (11/1/09 – 4/30/10)
4 New Version / Revision and Final Review (5/1/10 – 8/31/10)
5 Discuss New Version / Revision (9/30/10)
COMMUNITY MEETING
PCI

Changes to the standard follow a defined 24-month lifecycle with five stages, described below. The lifecycle ensures a gradual, phased use of new versions of the standard without invalidating current implementations of PCI DSS or putting any organization out of compliance the moment changes are published. With the release of PCI DSS version 1.2 on October 1, 2008, the Council is committed to following this process to ensure transparency and continuity of compliance. The Council will publish similar lifecycles for the Payment Application Data Security Standard (PA-DSS) and the PIN Entry Device (PED) Security Requirements.

1: MONTHS 0–9
10/1/08 – 6/30/09

- Communications, implementation and dissemination of release
- Evaluate immediate feedback as needed

Stage 1: Market Implementation

The first nine months after release of the latest PCI DSS allows for market assessment and implementation. There is no *formal* feedback mechanism for proposed changes during Stage 1. Instead, this period allows merchants and other organizations time to plan and address standard-mandated changes, including lead times for sunset and expiration dates. The Council may accept and review comments received during Stage 1 to ensure there are no errors requiring an errata statement of clarification. During this stage, the Council will also ensure that supporting documentation is updated and available in multiple languages.

2: MONTHS 10–12
7/1/09 – 10/31/09

- Open formal feedback process
- Feedback compiled

Stage 2: Feedback Begins

The second stage allows for market input into evolving PCI DSS through a formal feedback process. Participating organizations and stakeholders will have the opportunity to *formally* express their views on the current version and provide suggestions for changes and improvements – especially in light of evolving technology and threats affecting cardholder data. The Council will clearly communicate with all stakeholders the process of how to submit feedback during this stage. The feedback phase eventually culminates with the next community meeting whereby feedback can be discussed in an open forum and compiled for systematic evaluation by the Council.

3: MONTHS 13–20
11/1/09 – 4/30/10

- Communicate compiled feedback
- Discuss feedback for community meeting
- Analyze trends and concern areas
- Evaluate impact
- Propose changes
- Determine action plan
- Issue preliminary draft to advisors for review

Stage 3: Feedback Review and Decision

During the eight-month third stage, the Council will compile feedback from many sources, including the participating organizations, assessment (QSA & ASV) community, Board of Advisors meetings, and community meetings. The Council's PCI DSS Technical Working Group (TWG) will systematically analyze the feedback, which will result in one of these actions:

- No action – if feedback does not warrant revising the standard
- Issuance of new version of PCI DSS (e.g., version 2.0, etc.)
- Issuance of revisions to PCI DSS (e.g., version 1.3, etc.)
- Development of new documentation to support the current version (e.g., whitepapers, best practices, additional FAQs, informational supplements, etc.)

No action terminates the lifecycle process at this point. Other actions will be communicated to stakeholders via various channels, such as email, newsletters, press releases, conference calls and Webinars.

If a revision or new version is required, the TWG will create a preliminary draft and present it for review and approval by the Board of Advisors and the Council's Executive Committee. The Council will clearly communicate all significant changes and/or sunset dates of current practices, along with timeframes for implementing newly specified best practices and/or requirements. This includes supporting documentation to ensure a smooth transition for compliance.

4: MONTHS 21–24
5/1/10 – 8/31/10

- Provide stakeholders summary of changes
- Provide new version or revision
- Provide lead times for new requirements

Stage 4: New Version / Revision and Final Review

The forth stage of the lifecycle allows the Council to finalize the new version or revision of PCI DSS and prepare for its formal release. During this three-month process, the Council will provide a "summary of changes" document to the stakeholder community with clear, precise guidance on what to expect in the new standard. The Council will also announce the date of issuance, which will close out the lifecycle process.

The new PCI DSS and its requirements will become effective immediately upon its publication on the Council's Web site at www.pcisecuritystandards.org.

Some new requirements may include phased implementation dates, which will provide merchants, other organizations and stakeholders with adequate time to implement required new systems or procedural changes. The Council will provide everyone with details well in advance, including phased implementation deadline dates, any subsequent sunset dates of current requirements or sub-requirements, or items affected by the revision update process. Sunset dates will usually be at least three months after publication of the updated standard. Once the sunset period passes, PCI DSS assessments will reflect requirements of the updated standard.

5: MONTH 24
9/30/10

- Revision or new version is effective immediately
- Provide guidance for those in the middle of an assessment
- Help organizations stay in compliance

Stage 5: Discuss New Version / Revision

Discussion of the new or revised PCI DSS occurs at the next community meeting. During this event, stakeholders can obtain more clarification and education to assist in implementing the updated standard. Discussion will also benefit the assessment community by helping them clearly understand changes to the standard and how this impacts assessments.