Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

Lifecycle Statement

Since its inception, the PCI Security Standards Council has worked to ensure that the development of the PCI DSS and other PCI security standards balances the need to evolve to face the challenges of a rapidly changing security landscape with the need for constancy. With that in mind, the Council is implementing a 24 month lifecycle review and change process. This means that that the PCI DSS will be refreshed every 24 months to provide clarity and flexibility where necessary and to address new or evolving data security threats/vulnerabilities as they emerge. This new standards lifecycle process addresses version control, timing and differences between versions (e.g., 2.0) and revisions (e.g., 1.2). This process is being implemented with the publication of version 1.2 of the PCI DSS, scheduled for October 1, 2008.

Specifically, when providing final communications regarding the changes, the Council will differentiate between substantive and minor clarification in the labeling of the Standard. A minor change, non-substantial in nature, or clarifications will result in a new revision. For example, the current version 1.1 will become 1.2. If there are new requirements or a significant change, then the new version would be released. For example version 1.2 would become version 2.0. In the future, when the Council issues a new version of the Standard (e.g., 2.0), any new requirements will be phased in with future effective dates to ensure the necessary time frames for compliance can be achieved. Regardless of whether changes to the PCI DSS result in a new version or revision, the timeline for any update will be on a two year cycle. However, depending on the critical nature of any proposed changes, the timeline might either be accelerated or delayed as needed.

It is important to note that the Council's intention is to foster ease of implementation and not place any merchant or service provider out of compliance through the issuance of a revision to the Standard. Notification of revisions to the PCI DSS will be publicly provided in advance of the changes being formalized. In addition, ample time for training and educating QSAs and ASVs on the new update will be provided.

Version 1.2
This most recent revision of the PCI DSS will not introduce any new requirements beyond the existing 12 that are already in place. Therefore version 1.2 will become effective immediately upon public release, currently scheduled for October 1, 2008. The sunset date for version 1.1 has not yet been determined, but will be at a minimum three months after the publication date. The published sunset date will signify that all new PCI DSS assessments must be conducted using the latest version or revision.

The upgrade to version 1.2 is for the PCI DSS only. The recently announced Payment Application Data Security Standard and PIN Entry Device Security Requirements will have their own lifecycle process. It is the Council's goal to synchronize the lifecycle for these standards with the PCI DSS lifecycle as outlined above. These additional standards are supportive of the PCI DSS and any updates to them will be based on the latest PCI DSS version. More information and details about the PCI DSS lifecycle process will be published on the Council's Web site in the coming weeks.