

PCI DSS v. 1.2 Summary of Changes
Frequently Asked Questions
FINAL

Q. Who has been providing feedback on the draft standards since you announced version 1.2 in May?

A. Council Participating Organizations and the Board of Advisors review and provide feedback on draft standards and revisions to existing standards. This is the key benefit of joining the Council as a Participating Organization.

Q. Why are you providing a “summary of changes” to the PCI DSS?

A. We believe it is necessary to have constant communication with stakeholders. While version 1.2 does not introduce any new, major requirements, we want to provide as much guidance as possible as to what will be included in this revision so that organizations can begin to prepare for any internal changes they might need to undergo.

Q. Does this mean that version 1.2 will put merchants out of compliance the moment it is released?

A. No. Where appropriate, the Council will provide ample lead time for organizations to make any needed changes to the security practices. In addition, an organization does not need to take immediate action to address any changes. Instead, those changes will be addressed during the organization's next scheduled PCI DSS assessment.

Q. How long can I continue using version 1.1 of the PCI DSS? What if I am in the middle of an assessment and will not be completed until after the expiration date? Can I complete my assessment using version 1.1?

A. If you have not started a new assessment then you can use version 1.1 of the PCI DSS for assessment purposes up to the sunset date published by the Council. Further, if you are currently in the process of an assessment using 1.1 you may continue to do so. The sunset date for version 1.1 has not yet been determined, but will be at a minimum three months after the publication date. Once the sunset date has been published, that timeframe and date will signify that all new PCI DSS assessments must be conducted using the latest version or revision

Q. I understand that a new revision of PCI DSS will be available in October 2008. What is the sunset date of the current version 1.1 and the effective date of the new revision?

A. Version 1.2 of the PCI DSS is a revision to the standard that does not introduce any new requirements. 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.

Q. Why are you doing this now by introducing these clarifications? Why not wait until a new version is introduced?

A. The Council has adopted a two year lifecycle process for PCI DSS and it is expected that a similar process will be used for the other standards it manages.

These clarifications are intended to make it easier for organizations to implement PCI DSS and we will continue to evaluate feedback and consider future revisions and changes in the same manner.

Q. I am not a Participating Organization. Why wasn't I able to comment and provide feedback on the draft revisions?

A. Only Participating Organizations can provide feedback. You can become one by visiting the Council's Web site or emailing the Council at participation@pcisecuritystandards.org.

Q. I understand you will be discussing version 1.2 at your upcoming Community Meetings. How can I register for one of these meetings?

A. Only Participating Organizations, QSAs, ASVs and PA-QSAs are able to attend the PCI SSC Community Meetings. You can contact the Council on joining as a Participating Organization at participation@pcisecuritystandards.org or by visiting our Web site.