

PCI DSS 1.2 FAQs
Updated: Oct. 21, 2008

Q. Who has been providing feedback on the draft standards since you announced version 1.2 in May and released it on Oct. 1, 2008?

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 did you provide a "summary of changes" to the PCI DSS prior to general availability on Oct. 1, 2008?

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 has been included in this revision so that organizations were better able 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. Why are you introducing clarifications in the version 1.2 revision to the standard? Why not wait until a new version 2.0 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. Version 1.2 is 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: The PCI DSS v. 1.2 announcement states that the new version goes into effect immediately and v. 1.1 sunsets Dec. 31, 2008. I am starting or in middle of my PCI DSS assessment right now, what impact does this have on me?

A. The effective date of the new standard is October 1, 2008, and the sunset date of the old standard is December 31, 2008. Assessments started prior to October 1 will be according to v. 1.1 and can be completed with v. 1.1. For assessments started between October 1 and December 31, either version can be used. For assessments started after December 31, version 1.2 must be used. The Council is not setting a date after which assessments against v. 1.1 will not be accepted since that is a compliance decision that is up to each payment brand. Please check with your acquirer or the payment brands for any final dates by which v. 1.1 assessments must be complete.

Q: My QSA is working with Version 1.1 as we are currently going through a PCI DSS assessment. Should we be telling them to use Version 1.2?

A. The effective date of the new standard is October 1, 2008, and the sunset date of the old standard is December 31, 2008. Assessments started prior to October 1 will be according to v. 1.1 and can be completed with v. 1.1. For assessments

started between October 1 and December 31, either version can be used. For assessments started after December 31, version 1.2 must be used. The Council is not setting a date after which assessments against v. 1.1 will not be accepted since that is a compliance decision that is up to each payment brand. Please check with your acquirer or the payment brands for any final dates by which v. 1.1 assessments must be complete. Your assessor should be aware of these requirements.

Q: I self assess compliance with PCI DSS and I am currently underway with a 1.1 assessment using the SAQ. What does the sunset date mean for me?

A. The effective date of the new standard is October 1, 2008, and the sunset date of the old standard is December 31, 2008. Assessments started prior to October 1 will be according to v. 1.1 and can be completed with v. 1.1. For assessments started between October 1 and December 31, either version can be used. For assessments started after December 31, version 1.2 must be used. The Council is not setting a date after which assessments against v. 1.1 will not be accepted since that is a compliance decision that is up to each payment brand. Please check with your acquirer or the payment brands for any final dates by which v. 1.1 assessments must be complete. The SAQs for v. 1.2 will be available by the middle of November 2008.

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. Our Community Meeting in Orland, Fla., was attended by nearly 600 individuals all with the same mission – to protect cardholder data. There is an additional Community meeting being held in Brussels, Belgium, Oct. 21-23. You can contact the Council on joining as a Participating Organization at participation@pcisecuritystandards.org or by visiting our Web site.