PCI DSS 3.2 Resource Guide

The Payment Card Industry Security Standards Council (PCI SSC) has published a new version of the industry standard that businesses use to safeguard payment data before, during and after purchase. PCI Data Security Standard (PCI DSS) version 3.2 replaces version 3.1 to address growing threats to customer payment information. Companies that accept, process or receive payments should adopt it as soon as possible to prevent, detect and respond to cyberattacks that can lead to breaches. Read on for answers to key questions about updates to the standard, timelines, and resources available for understanding and adopting PCI DSS version 3.2.

Q Why is the PCI DSS being updated?

A: The Council updates the PCI DSS to ensure it continues to protect against old exploits that are still causing problems, addresses new exploits and provides greater clarity for implementing and maintaining PCI DSS controls.

Q Why is it PCI DSS 3.2 and not PCI DSS 4.0?

A: The industry recognizes PCI DSS as a mature standard now, which doesn't require the significant updates we have seen in the past. Moving forward, the marketplace can expect incremental revisions like 3.2 to address the changing threat and payment landscape, with a focus on providing clarity and guidance to help companies use and maintain the standard as everyday business practice.

Q What are the types of changes included in PCI DSS 3.2?

A: PCI DSS 3.2 includes clarifications to existing requirements, new or evolving requirements, and additional guidance. These are outlined in the Summary of Changes from PCI DSS 3.1 to PCI DSS 3.2.

Q What is new in PCI DSS 3.2?

A: Within the 12 core requirements of the PCI DSS, there are five new sub-requirements for service providers affecting requirements 3, 10, 11 and 12. New sub-requirements have been added to requirement 8 to ensure multi-factor authentication is used for all non-console administrative access and all remote access in the cardholder data environment. There are also two new appendices. Appendix A2 incorporates new migration deadlines for removal of Secure Sockets Layer (SSL) /early Transport Layer Security (TLS) in line with the December 2015 bulletin. Appendix A3 incorporates the "Designated Entities Supplemental Validation" (DESV), which was previously a separate document. All the changes are outlined in the Summary of Changes from PCI DSS 3.1 to PCI DSS 3.2.

Q How are these changes determined?

A: The standard update is part of the regular process for ensuring the PCI DSS addresses current challenges and threats. This process factors in industry feedback from the PCI Council's more than 700 global Participating Organizations, as well as data breach report findings and changes in payment acceptance.

Q How long do organizations have to implement PCI DSS 3.2?

A: PCI DSS 3.1 will retire on 31 October 2016, and after this time all assessments will need to use version 3.2. Between now and 31 October 2016, either PCI DSS 3.1 or 3.2 may be used for PCI DSS assessments. The new requirements introduced in PCI DSS 3.2 are considered best practices until 31 January 2018. Starting 1 February 2018 they are effective as requirements and must be used.

Q What supporting documentation is available for compliance with PCI DSS 3.2?

A: PCI DSS 3.2 supporting documents include updated Self-Assessment Questionnaires (SAQ), Attestation of Compliance (AOC) forms, Report on Compliance (ROC) templates, Frequently Asked Questions (FAQ) and Glossary. All of these are available in the Documents Library on the PCI SSC website.

Q Are PCI Training courses updated for PCI DSS 3.2?

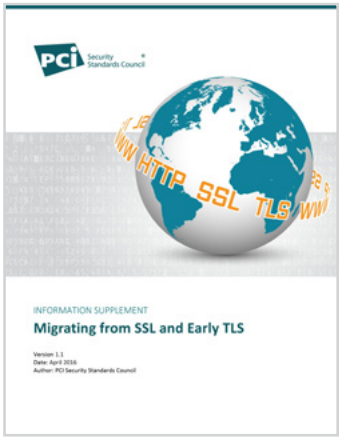
A: Yes, content for all PCI Training programs is being updated to support PCI DSS 3.2.

RESOURCES

Summary of Changes from PCI DSS Version 3.1 to 3.2

PCI DSS 3.2 Highlights Webinar

Glossary



Migrating from SSL/Early TLS Information Supplement

Media: for expert comment please contact: press@pcisecuritystandards.org
For more information on PCI Standards and resources, visit: www.pcisecuritystandards.org