Payment Card Industry (PCI)

Data Security Standard

Summary of Changes from PCI DSS Version 3.2 to 3.2.1

May 2018

Introduction

This document provides a summary of changes from PCI DSS v3.2 to PCI DSS v3.2.1. Table 1 provides an overview of the types of changes. Table 2 summarizes the material changes found in PCI DSS v3.2.1.

Table 1: Change Types

[1]Change Type	Definition
Clarification	Clarifies intent of requirement. Ensures that concise wording in the standard portrays the desired intent of requirements.
Additional guidance	Explanation, definition and/or instruction to increase understanding or provide further information or guidance on a particular topic.
Evolving Requirement	Changes to ensure that the standards are up to date with emerging threats and changes in the market.

Table 2: Summary of Changes

Section		Change	Type[1]
PCI DSS v3.2	**PCI DSS v3.2.1**		
Various	Various	Addressed minor punctuation and format issues.	Clarification
PCI DSS Versions	PCI DSS Versions	Updated to describe how this version of PCI DSS impacts the previous version.	Clarification
Requirements			
2.2.3 2.3 4.1	2.2.3 2.3 4.1	Removed note and testing procedure regarding use of Appendix A2 to report SSL/early TLS migration effort, as the migration date has passed. Added note to guidance referencing updated applicability of Appendix A2.	Clarification
3.5.1 6.4.6 8.3.1 10.8, 10.8.1 11.3.4.1 12.4.1 12.11, 12.11.1	3.5.1 6.4.6 8.3.1 10.8, 10.8.1 11.3.4.1 12.4.1 12.11, 12.11.1	Removed note from requirements referring to an effective date of February 1, 2018, as this date has passed.	Clarification
3.6.2	3.6.2	Fixed error in Guidance Column: Reference to Requirement 3.5.1 changed to 3.5.2.	Clarification
Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS	Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI terminal connections	Updated Appendix A2 to reflect that the SSL/early TLS migration date of July 1, 2018 has passed. Requirements A2.1 – A2.3 updated to focus only on the allowance for POS POIs that are not susceptible to known exploits and their service provider termination points to continue using SSL/early TLS.	Clarification
Appendix B: Compensating Controls	Appendix B: Compensating Controls	Replaced reference to Navigating Guide with Guidance Column for understanding intent of requirements. Removed MFA from the compensating control example, as MFA is now required for all non-console administrative access. Added use of one time passwords as an alternative potential control for this scenario.	Clarification