Payment Card Industry (PCI)

Data Security Standard

Summary of Changes from PCI DSS Version 3.0 to 3.1

April 2015

Introduction

This document provides a summary of changes from PCI DSS v3.0 to PCI DSS v3.1. Table 1 provides an overview of the types of changes. Table 2 summarizes the material changes found in PCI DSS v3.1.

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 v3.0	**PCI DSS v3.1**		
All	All	Addressed minor typographical errors (grammar, punctuation, formatting, etc.) and incorporated minor updates for readability throughout the document.	Clarification
Introduction	Introduction	Changed reference from "protecting cardholder data" to "protecting account data".	Clarification
Introduction	Introduction	Clarified that PCI DSS applies to *any* entity that stores, processes or transmits account data.	Clarification
Introduction	Introduction	Changed reference from "personally identifiable information" to "personal information".	Clarification
PCI DSS Applicability Information	PCI DSS Applicability Information	Changed reference from "financial institutions" to "acquirers, issuers".	Clarification
PCI DSS Applicability Information	PCI DSS Applicability Information	Removed reference to "environments" to clarify applicability at the organization level rather than the system level.	Clarification
Scope of PCI DSS Requirements	Scope of PCI DSS Requirements	Aligned with language used earlier in the same section regarding steps for confirming accuracy of the defined CDE.	Clarification
Use of Third Party Service Providers / Outsourcing	Use of Third Party Service Providers / Outsourcing	Clarified that validation processes for service providers include undergoing their own annual assessments or undergoing multiple on-demand assessments.	Clarification
PCI DSS Assessment Process	PCI DSS Assessment Process	Reordered assessment steps to clarify that a ROC, SAQ, or AOC may be submitted without all requirements being "in place".	Clarification
General	General	Updated language in requirements and/or testing procedures for consistency.	Clarification
2.2.3	2.2.3	Removed SSL as an example of a secure technology. Added note that SSL and early TLS are no longer considered to be strong cryptography and cannot be used as a security control after June 30, 2016. Additional guidance provided in Guidance column. Also impacts Requirements 2.3 and 4.1.	Evolving Requirement
2.3	2.3	Removed SSL as an example of a secure technology and added a note to the requirement. See explanation above at 2.2.3.	Evolving Requirement

3.2.1 – 3.2.3	3.2.1 – 3.2.3	Clarified in requirements that storage of sensitive authentication data is not permitted "after authorization".	Clarification
3.4	3.4	Clarified in requirement note that additional controls are required if hashed and truncated versions of the same PAN are present in an environment. Added Testing Procedure 3.4.e to assist with validation of the Note. Clarified intent of "truncation" in Guidance Column.	Clarification
3.5.2	3.5.2	Clarified that "HSM" may refer to a "Hardware" or "Host" Security Module. Aligned with language in PCI PTS.	Clarification
3.6	3.6	Clarified that Testing Procedure 3.6.a only applies if the entity being assessed is a service provider.	Clarification
4.1	4.1	Removed SSL as an example of a secure technology and added a note to the requirement. See explanation above at 2.2.3.	Evolving Requirement
4.1.1	4.1.1	Updated testing procedure to recognize all versions of SSL as examples of weak encryption.	Evolving Requirement
4.2	4.2	Included SMS as an example of end-user messaging technology and added guidance.	Clarification Additional Guidance
6.6	6.6	Added clarification to testing procedure and Guidance column that if an automated technical solution is configured to alert (rather than block) web-based attacks, there must also be a process to ensure timely response.	Clarification
8.1.4	8.1.4	Clarified that inactive user accounts must be removed/disabled *within* 90 days.	Clarification
8.1.6.b 8.2.1.d 8.2.1.e 8.2.3.b 8.2.4.b 8.2.5.b	8.1.6.b 8.2.1.d 8.2.1.e 8.2.3.b 8.2.4.b 8.2.5.b	Clarified that Testing Procedure only applies if the entity being assessed is a service provider, and for non-consumer customer accounts.	Clarification
8.2.4	8.2.4	Clarified that passwords must be changed at least *once* every 90 days.	Clarification
8.5.1	8.5.1	Clarified this requirement only applies if the entity being assessed is a service provider.	Clarification

9.2	9.2	Clarified that the requirement applies to all onsite personnel and visitors. Combined Testing Procedures 9.2.b and 9.2.d to remove redundancy.	Clarification
9.9.1.b	9.9.1.b	Updated testing procedure to clarify both devices and device locations need to be observed.	Clarification
10.6	10.6	Removed redundant language in guidance column.	Clarification
10.6.1	10.6.1	Updated requirement to more clearly differentiate intent from Requirement 10.6.2.	Clarification
11.1.c	11.1.c	Clarified that testing procedure applies where wireless scanning is utilized.	Clarification
11.2	11.2	Clarified in Guidance Column that a vulnerability scan could be a combination of automated and manual tools, techniques, or other methods.	Additional Guidance
11.3.2.a	11.3.2.a	Removed redundant language from testing procedure.	Clarification
11.3.4	11.3.4	Clarified that the intent of the penetration testing is to verify that all out-of-scope systems are segmented (isolated) from systems “in the CDE”.	Clarification
11.5	11.5	Clarified that unauthorized modifications include changes, additions, and deletions of critical system files, etc.	Clarification
12.2	12.2	Clarified that the risk assessment process must result in a formal, “documented analysis of risk”.	Clarification
12.9	12.9	Clarified this requirement only applies if the entity being assessed is a service provider and added related guidance.	Clarification Additional Guidance
Appendix C: Compensating Controls Worksheet – Completed Example	Appendix C: Compensating Controls Worksheet – Completed Example	Updated description of compensating control example to reflect use of “sudo” rather than “SU” for improved technical accuracy.	Additional Guidance