Payment Card Industry (PCI)

Data Security Standard

Summary of Changes from PCI DSS Version 3.1 to 3.2

April 2016

Introduction

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

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 v3.1	**PCI DSS v3.2**		
All	All	Addressed minor typographical errors (grammar, punctuation, formatting, etc.) and incorporated minor updates for readability throughout the document.	Clarification
Relationship between PCI DSS and PA-DSS	Relationship between PCI DSS and PA-DSS	Added guidance that security threats are constantly evolving, and payment applications that are not supported by the vendor may not offer the same level of security as supported version.	Additional guidance
Scope of PCI DSS Requirements	Scope of PCI DSS Requirements	Clarified that backup/recovery sites need to be considered when confirming PCI DSS scope.	Clarification
Best Practices for Implementing PCI DSS into Business-as-Usual Processes	Best Practices for Implementing PCI DSS into Business-as-Usual Processes	Updated Note to clarify that some business-as-usual principles may be requirements for certain entities, such as those defined in the Designated Entities Supplemental Validation (Appendix A3).	Clarification
	PCI DSS Versions	New section to describe how this version of PCI DSS impacts the previously-effective version.	Additional guidance
Requirements			
General	General	Removed examples of “strong” or “secure” protocols from a number of requirements, as these may change at any time.	Clarification
General	General	Moved examples from a number of requirements and/or testing procedures to the Guidance column, and added guidance where appropriate.	Clarification
General	General	Changed “passwords/phrases” to “passwords/passphrases” in a number of requirements for consistency.	Clarification
General	General	Clarified correct term is multi-factor authentication, rather than two-factor authentication, as two or more factors may be used.	Clarification
General	General	Removed notes from requirements referring to an effective date of July 1, 2015, as these are now effective. Affected requirements are 6.5.10, 8.5.1, 9.9, 11.3, and 12.9.	Clarification
1.1.6	1.1.6	Clarified that approval of business use is included in the justification. Removed examples of “insecure” protocols as these may change in accordance with industry standards.	Clarification

Section		Change	Type[1]
PCI DSS v3.1	PCI DSS v3.2		
1.2.1	1.2.1	Added guidance to clarify intent of requirement.	Clarification
1.3	1.3	Added guidance to clarify intent of requirement.	Clarification
1.3.3		Removed requirement as intent is addressed via other requirements in 1.2 and 1.3.	Clarification
1.3.4 – 1.3.8	1.3.3 – 1.3.7	Renumbered due to removal of former Requirement 1.3.3.	Clarification
1.3.6	1.3.5	Updated to clarify intent of requirement rather than use of a particular type of technology.	Clarification
1.4	1.4	Increased flexibility by including *or equivalent functionality* as alternative to personal firewall software. Clarified requirement applies to all portable computing devices that connect to the Internet when outside the network and that also access the CDE.	Clarification
2.1	2.1	Clarified requirement applies to payment applications.	Clarification
2.2.3	2.2.3	Removed note and testing procedures regarding removal of SSL/early TLS and moved to new Appendix A2.	Clarification
2.3	2.3	Removed note and testing procedures regarding removal of SSL/early TLS and moved to new Appendix A2. Removed reference to “web-based management” as requirement already specifies “all non-console administrative access”, which by definition includes any web-based access.	Clarification
3.3	3.3	Updated requirement to clarify that any displays of PAN greater than the first six/last four digits of the PAN requires a legitimate business need. Added guidance on common masking scenarios.	Evolving Requirement
3.4.d	3.4.d	Updated testing procedure to clarify the examination of audit logs includes payment application logs.	Clarification
3.4.1	3.4.1	Added note to requirement to clarify the requirement applies in addition to all other PCI DSS encryption and key management requirements.	Clarification

Section		Change	Type[1]
PCI DSS v3.1	PCI DSS v3.2		
	3.5.1	New requirement for service providers to maintain a documented description of the cryptographic architecture. *Effective February 1, 2018*	Evolving Requirement
3.5.1 – 3.5.3	3.5.2 – 3.5.4	Renumbered due to addition of new Requirement 3.5.1.	Clarification
3.6.1.b	3.6.1.b	Updated testing procedure language to clarify testing involves observation of procedures rather than key-generation method itself, as this should not be observable. Added guidance referring to Glossary definition for "Cryptographic Key Generation"	Clarification
4.1	4.1	Removed note and testing procedures regarding removal of SSL/early TLS and moved to new Appendix A2.	Clarification
6.2	6.2	Added clarification to Guidance column that requirement to patch all software includes payment applications.	Clarification
6.4.4	6.4.4	Updated requirement to align with testing procedure.	Clarification
6.4.5	6.4.5	Clarified that change control processes are not limited to patches and software modifications.	Clarification
	6.4.6	New requirement for change control processes to include verification of PCI DSS requirements impacted by a change. *Effective February 1, 2018*	Evolving Requirement
6.5	6.5	Clarified that training for developers must be up to date and occur at least annually.	Clarification
6.5.a – 6.5.d	6.5.a – 6.5.c	Removed Testing Procedure 6.5.b and renumbered remaining testing procedures to accommodate.	Clarification
7.2	7.2	Updated requirement, testing procedures and Guidance column to clarify that one or more access control systems may be used.	Clarification
Requirement 8	Requirement 8	Added note to Requirement 8 introduction that the authentication requirements do not apply to accounts used by consumers (e.g. cardholders).	Clarification
8.1.5	8.1.5	Clarified requirement intended for all third parties with remote access, rather than only vendors.	Clarification

Section		Change	Type[1]
PCI DSS v3.1	PCI DSS v3.2		
8.2.3	8.2.3	Updated Guidance column to reflect changing industry standards.	Clarification
8.3	8.3	Clarified correct term is multi-factor authentication rather than two-factor authentication, as two or more factors may be used.	Clarification
8.3	8.3, 8.3.1, 8.3.2	Expanded Requirement 8.3 into sub-requirements, to require multi-factor authentication for all personnel with non-console administrative access, and all personnel with remote access to the CDE. New Requirement 8.3.2 addresses multi-factor authentication for all personnel with remote access to the CDE (incorporates former Requirement 8.3). New Requirement 8.3.1 addresses multi-factor authentication for all personnel with non-console administrative access to the CDE. *Requirement 8.3.1 effective February 1, 2018*	Evolving Requirement
9.1.1	9.1.1	Clarified that either video cameras or access controls mechanisms, or both, may be used.	Clarification
9.5.1.a – 9.5.1.b	9.5.1	Combined testing procedures to clarify that assessor verifies the storage location is reviewed at least annually.	Clarification
	10.8, 10.8.1	New requirement for service providers to detect and report on failures of critical security control systems. *Effective February 1, 2018*	Evolving Requirement
10.8	10.9	Renumbered due to addition of new Requirement 10.8.	Clarification
11.2.1	11.2.1	Clarified that all “high risk” vulnerabilities must be addressed in accordance with the entity’s vulnerability ranking (as defined in Requirement 6.1), and verified by rescans.	Clarification
11.3.4	11.3.4	Added Testing Procedure 11.3.4.c to confirm penetration test is performed by a qualified internal resource or qualified external third party.	Clarification
	11.3.4.1	New requirement for service providers to perform penetration testing on segmentation controls at least every six months. *Effective February 1, 2018*	Evolving Requirement

Section		Change	Type[1]
PCI DSS v3.1	**PCI DSS v3.2**		
11.5.a	11.5.a	Removed "within the cardholder data environment" from testing procedure for consistency with requirement, as requirement may apply to critical systems located outside the designated CDE.	Clarification
12.3.3	12.3.3	Reformatted testing procedure for clarity.	Clarification
	12.4	New requirement for service providers' executive management to establish responsibilities for the protection of cardholder data and a PCI DSS compliance program. *Effective February 1, 2018*	Evolving Requirement
12.4	12.4.1	Renumbered due to addition of new Requirement 12.4.	Clarification
12.6	12.6	Clarified intent of security awareness program is to ensure personnel are aware of the cardholder data security policy and procedures.	Clarification
12.8.1	12.8.1	Clarified that the list of service providers includes a description of the service provided.	Clarification
12.8.2	12.8.2	Added guidance that service provider responsibility will depend on the particular service being provided and the agreement between the two parties.	Additional Guidance
12.10.2	12.10.2	Clarified that review of the incident response plan encompasses all elements listed in Requirement 12.10.1.	Clarification
	12.11, 12.11.1	New requirement for service providers to perform reviews at least quarterly, to confirm personnel are following security policies and operational procedures. *Effective February 1, 2018*	Evolving Requirement
Appendix A	Appendix A1	Renumbered Appendix "*Additional PCI DSS Requirements for Shared Hosting Providers*" due to inclusion of new appendices.	Clarification
	Appendix A2	New Appendix with additional requirements for entities using SSL/early TLS, incorporating new migration deadlines for removal of SSL/early TLS.	Clarification
	Appendix A3	New Appendix to incorporate the "Designated Entities Supplemental Validation" (DESV), which was previously a separate document.	Clarification