Payment Card Industry (PCI)

Data Security Standard

Summary of Changes from PCI DSS Version 2.0 to 3.0

November 2013

Introduction

This document provides a summary of changes from PCI DSS v2.0 to PCI DSS v3.0. Table 1 provides an overview of the types of changes included in PCI DSS v3.0. Table 2 provides a summary of material changes to be found in PCI DSS v3.0.

Table 1: Change Types

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
PCI DSS v2.0	**PCI DSS v3.0**		
PCI DSS Applicability Information	PCI DSS Applicability Information	Clarified that SAD must not be stored after authorization even if there is no PAN in the environment.	Clarification
Relationship between PCI DSS and PA-DSS	Relationship between PCI DSS and PA-DSS	Clarified that all applications that store, process, or transmit cardholder data are in scope for an entity's PCI DSS assessment, even if PA-DSS validated. Clarified PCI DSS applicability to payment application vendors.	Clarification
Scope of Assessment for Compliance with PCI DSS Requirements	Scope of PCI DSS Requirements	Added examples of system components, and added guidance about how to accurately determine the scope of the assessment. Clarified the intent of segmentation. Clarified responsibilities of both the third party and their customers for scoping and coverage of PCI DSS requirements, and clarified the evidence that third parties are expected to provide for their customers to be able to verify the scope of the third party's PCI DSS assessment.	Additional Guidance
	Implementing PCI DSS into Business-as-Usual Processes	New section to provide "business as usual" guidance for implementing security into business-as-usual (BAU) activities to maintain on-going PCI DSS compliance. Note that this section includes recommendations and guidance only, not new PCI DSS requirements.	Additional Guidance
	Assessment Procedures	Added new heading to separate PCI DSS scoping section from sampling section.	Clarification
Sampling of Business Facilities/System Components	For Assessors: Sampling of Business Facilities/System Components	Enhanced sampling guidance for assessors.	Additional Guidance
Instructions and Content for Report on Compliance	Instructions and Content for Report on Compliance	Former content relocated to separate documents – PCI DSS ROC Template and PCI DSS ROC Reporting Instructions.	Clarification
PCI DSS Compliance – Completion Steps	PCI DSS Assessment Process	Updated section to focus on assessment process rather than documentation.	Clarification
Detailed PCI DSS Requirements and Security Assessment Procedures	Detailed PCI DSS Requirements and Security Assessment Procedures	At the start of this section, added language to define the column headings in this section, and removed references to "In Place," "Not In Place" and "Target Date/Comments" columns.	Clarification

General changes implemented throughout the PCI DSS requirements	Type
New column to describe the intent of each requirement, with content derived from former Navigating PCI DSS guidance document. The guidance in this column is intended to assist understanding of the requirements and does not replace or extend the PCI DSS Requirements and Testing Procedures.	Additional Guidance
For the security policies and daily operational procedures (formerly requirements 12.1.1 and 12.2), assigned a new requirement number and moved requirements and testing procedures into each of Requirements 1-11.	Clarification
Updated language in requirements and/or corresponding testing procedures for alignment and consistency.	Clarification
Separated complex requirements / testing procedures for clarity and removed redundant or overlapping testing procedures.	Clarification
Enhanced testing procedures to clarify level of validation expected for each requirement.	Clarification
Other general editing changes include: • Removed the following columns: "In Place", "Not in Place" and "Target Date/Comments". • Renumbered requirements and testing procedures to accommodate changes • Reformatted requirements and testing procedures for readability – e.g. content from paragraph reformatted to bullet points, etc. • Made minor wording changes throughout for readability • Corrected typographical errors	

Requirement		Change	Type
PCI DSS v2.0	PCI DSS v3.0		
Requirement 1			
1.1.x	1.1.x	Clarified that firewall and router standards have to be both documented and implemented.	Clarification
1.1.2	1.1.2 1.1.3	Clarified what the network diagram must include and added new requirement at 1.1.3 for a current diagram that shows cardholder data flows.	Evolving Requirement
1.1.5	1.1.6	Clarified examples of insecure services, protocols, and ports to specify SNMP v1 and v2.	Clarification
1.2.2	1.2.2	Clarified that the intent of securing router configuration files is to secure them from unauthorized access.	Clarification
1.2.3	1.2.3	Clarified that the intent of controlling traffic between wireless networks and the CDE is to "permit only authorized traffic."	Clarification
1.3.4	1.3.4	Clarified the intent of the requirement is that anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the network.	Clarification

Requirement		Change	Type
PCI DSS v2.0	PCI DSS v3.0		
1.4	1.4	Aligned language between requirement and testing procedures for consistency.	Clarification
Requirement 2			
2.1	2.1	Clarified that requirement for changing vendor default passwords applies to all default passwords, including systems, applications, security software, terminals, etc. and that unnecessary default accounts are removed or disabled.	Clarification
2.1.1	2.1.1	Clarified that the intent of the requirement is for all wireless vendor defaults to be changed at installation.	Clarification
2.2	2.2	Clarified that system configuration standards include procedures for changing of all vendor-supplied defaults and unnecessary default accounts.	Clarification
2.2.2	2.2.2 2.2.3	Split requirement at 2.2.2 into two requirements to focus separately on *necessary* services, protocols and ports (2.2.2), and *secure* services, protocols, and ports (2.2.3).	Clarification
	2.4	New requirement to maintain an inventory of system components in scope for PCI DSS to support development of configuration standards.	Evolving Requirement
Requirement 3			
3.1 3.1.1	3.1	Combined requirement 3.1.1 and testing procedures into requirement 3.1 to clarify and reduce redundancy.	Clarification
3.2	3.2	Clarified, if sensitive authentication data is received, that it is rendered unrecoverable upon completion of the authorization process. Clarified testing procedures for companies that support issuing services and store sensitive authentication data.	Clarification
3.3	3.3	Clarified intent of requirement for masking PANs by consolidating former note into body of the requirement, and enhancing testing procedures.	Clarification
3.4.1	3.4.1	Clarified that logical access for disk encryption must be managed *separately* and independently of the native operating system *authentication* and access control mechanisms, and that decryption keys must not be *associated with* user accounts.	Clarification
3.5	3.5	Clarified that key management procedures have to be both implemented and documented.	Clarification

Requirement		Change	Type
PCI DSS v2.0	PCI DSS v3.0		
3.5.2	3.5.2 3.5.3	Split requirement 3.5.2 into two requirements to focus separately on storing cryptographic keys in a secure form (3.5.2), and in the fewest possible locations (3.5.3). Requirement 3.5.2 also provides flexibility with more options for secure storage of cryptographic keys.	Clarification
3.6.x	3.6.x	Added testing procedures to verify implementation of cryptographic key management procedures.	Clarification
3.6.6	3.6.6	Clarified principles of split knowledge and dual control.	Clarification
Requirement 4			
4.1	4.1	Aligned language between requirement and testing procedures for consistency. Also expanded the examples of open, public networks.	Clarification
Requirement 5			
Requirement 5 - General		Title updated to reflect intent of the requirement (to *protect all systems against malware).*	Clarification
	5.1.2	New requirement to evaluate evolving malware threats for any systems not considered to be commonly affected by malicious software.	Evolving Requirement
5.2	5.2	Aligned language between requirement and testing procedures for consistency.	Clarification
	5.3	New requirement to ensure that anti-virus solutions are actively running (formerly in 5.2), and cannot be disabled or altered by users unless specifically authorized by management on a per-case basis.	Evolving Requirement
Requirement 6			
6.2	6.1	Switched the order of requirements 6.1 and 6.2. Requirement 6.1 is now for identifying and risk ranking new vulnerabilities and 6.2 is for patching critical vulnerabilities. Clarified how risk ranking process (6.1) aligns with patching process (6.2).	Clarification
6.1	6.2	See above explanation for 6.1. Also, clarified that this requirement applies to “applicable” patches.	Clarification
6.3	6.3	Added a note to clarify that the requirement for written software development processes applies to all internally-developed software and bespoke software.	Clarification
6.3.1	6.3.1	Changed “pre-production” to “development/test” to clarify intent of requirement	Clarification

Requirement		Change	Type
PCI DSS v2.0	PCI DSS v3.0		
6.4	6.4	Enhanced testing procedures to include document reviews for all requirements at 6.4.1 through 6.4.4.	Clarification
6.4.1	6.4.1	Aligned language between requirement and testing procedures to clarify that separation of production/ development environments is enforced with access controls.	Clarification
6.5	6.5	Updated developer training to include how to avoid common coding vulnerabilities, and to understand how sensitive data is handled in memory.	Clarification
6.5.x	6.5.x	Updated requirements to reflect current and emerging coding vulnerabilities and secure coding guidelines. Updated testing procedures to clarify how the coding techniques address the vulnerabilities.	Clarification
	6.5.10	New requirement for coding practices to protect against broken authentication and session management. *Effective July 1, 2015*	Evolving Requirement
6.6	6.6	Increased flexibility by specifying *automated technical solution that detects and prevents web-based attacks* rather than "web-application firewall." Added note to clarify that this assessment is not the same as vulnerability scans required at 11.2.	Clarification
Requirement 7			
7.1	7.1	Reworded testing procedure to clarify what the policy includes, based on changes to requirements 7.1.1 through 7.1.4.	Clarification
	7.1.1	New 7.1.1 to cover definition of access needs for each role, to support requirements 7.1.2 through 7.1.4.	Clarification
7.1.1	7.1.2	Refocused requirement on restriction of privileged user IDs to least privileges necessary, and enhanced testing procedures.	Clarification
7.1.2	7.1.3	Refocused requirement on assignment of access based on individual's job classification and function.	Clarification
7.1.4		Removed former requirement 7.1.4 (covered in Requirement 7.2)	Clarification

Requirement		Change	Type
PCI DSS v2.0	PCI DSS v3.0		
Requirement 8			
Requirement 8 - General		Title updated to reflect intent of the requirement (identify and authenticate all access to system components). Updated and reorganized requirements to provide a more holistic approach to user authentication and identification: • Focused 8.1 on user identification • Focused 8.2 on user authentication • Updated requirements to consider methods of authentication other than passwords • Changed "passwords" to "passwords/phrases" where requirement only applies to passwords/phrases • Changed "passwords" to "authentication credentials" where requirement applies to any type of authentication credential • Clarified that password security requirements apply to accounts used by third party vendors	Clarification
8.5.6	8.1.5	Clarified the requirement for remote vendor access applies to vendors who access, support or maintain system components, and that it should be disabled when not in use.	Clarification
8.4.2	8.2.1	Clarified that strong cryptography must be used to render authentication credentials unreadable during transmission and storage.	Clarification
8.5.2	8.2.2	Clarified that user identify must be verified before modifying authentication credentials, and added provisioning new tokens and generating new keys as examples of modifications.	Clarification
8.5.10 8.5.11	8.2.3	Combined minimum password complexity and strength requirements into single requirement, and increased flexibility for alternatives that meet the equivalent complexity and strength.	Evolving Requirement
8.3	8.3	Clarified requirement for two-factor authentication applies to users, administrators, and all third parties, including vendor access for support or maintenance.	Clarification
8.5.7	8.4	Enhanced requirement to include documenting and communicating guidance for how users should protect their authentication credentials, including password/phrase reuse and changing password/phrase if there is suspicion that it has been compromised.	Clarification
	8.5.1	New requirement for service providers with remote access to customer premises, to use unique authentication credentials for each customer. *Effective July 1, 2015*	Evolving Requirement

Requirement		Change	Type
PCI DSS v2.0	**PCI DSS v3.0**		
	8.6	New requirement where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) that the mechanisms must be linked to an individual account and ensure only the intended user can gain access with that mechanism.	Evolving Requirement
8.5.16	8.7	Aligned language between requirement and testing procedures for consistency.	Clarification
Requirement 9			
9.1.2	9.1.2	Clarified intent of the requirement is to implement physical and/or logical access controls to protect publically-accessible network jacks.	Clarification
9.2.x	9.2.x	Clarified the intent of the requirement to identify, distinguish between, and grant access to onsite personnel and visitors, and that badges are just one option (they are not required).	Clarification
	9.3	New requirement to control physical access to sensitive areas for onsite personnel, including a process to authorize access, and revoke access immediately upon termination.	Evolving Requirement
9.3.x	9.4.x	Aligned language between requirement and testing procedures for consistency and to clarify that visitors must be escorted at all times, and that the audit trail of visitor activity must include access to the facility, computer room, and/or data center.	Clarification
9.5 – 9.10	9.5 – 9.8	Former requirement 9.6 moved and renumbered to 9.5, and former requirement 9.5 renumbered as sub-requirement 9.5.1. Former requirement 9.7 renumbered to 9.6, and former requirement 9.8 renumbered as sub-requirement 9.6.3. Former requirement 9.9 renumbered to 9.7, and former requirement 9.10 renumbered to 9.8.	Clarification
	9.9.x	New requirements to protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. *Effective July 1, 2015*	Evolving Requirement
Requirement 10			
10.1	10.1	Clarified that audit trails should be implemented to link access to system components to each individual user, rather than just establishing a process.	Clarification
10.2.1	10.2.1	Clarified the intent is for all individual *user* access to cardholder data to be included in the audit trails.	Clarification

Requirement		Change	Type
PCI DSS v2.0	PCI DSS v3.0		
10.2.5	10.2.5	Enhanced requirement to include changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions and deletions to accounts with root or administrative access.	Evolving Requirement
10.2.6	10.2.6	Enhanced requirement to include stopping or pausing of the audit logs.	Evolving Requirement
10.6	10.6.x	Clarified the intent of log reviews is to identify anomalies or suspicious activity, and provided more guidance about scope of daily log reviews. Also allowed more flexibility for review of security events and critical system logs daily and other logs events periodically, as defined by the entity's risk management strategy.	Clarification
Requirement 11			
11.1.x	11.1.x	Enhanced requirement to include an inventory of authorized wireless access points and a business justification (11.1.1) to support scanning for unauthorized wireless devices, and added new requirement 11.1.2 to align with an already-existing testing procedure, for incident response procedures if unauthorized wireless access points are detected.	Evolving Requirement
11.2	11.2	Added guidance on combining multiple scan reports in order to achieve and document a passing result.	Additional Guidance
11.2.1	11.2.1	Clarified that quarterly internal vulnerability scans include rescans as needed until all "high" vulnerabilities (as identified by PCI DSS Requirement 6.1) are resolved, and must be performed by qualified personnel.	Clarification
11.2.2	11.2.2	Clarified that external vulnerability scans include rescans as needed until passing scans are achieved, and added a note to refer to the ASV Program Guide.	Clarification
11.2.3	11.2.3	Clarified that internal and external scans performed after significant changes include rescans as needed until all "high" vulnerabilities (as identified by PCI DSS Requirement 6.1) are resolved, and must be performed by qualified personnel.	Clarification
	11.3	New requirement to implement a methodology for penetration testing. *Effective July 1, 2015. PCI DSS v2.0 requirements for penetration testing must be followed until v3.0 is in place.*	Evolving Requirement
11.3	11.3.1 11.3.2	Split former requirement 11.3 into 11.3.1 for *external* penetration testing requirements and 11.3.2 for *internal* penetration testing requirements.	Clarification

Requirement		Change	Type
PCI DSS v2.0	PCI DSS v3.0		
11.3	11.3.3	New requirement created from former testing procedure (11.3.b) to correct exploitable vulnerabilities found during penetration testing and repeat testing to verify corrections.	Clarification
	11.3.4	New requirement, if segmentation is used to isolate the CDE from other networks, to perform penetration tests to verify that the segmentation methods are operational and effective.	Evolving Requirement
11.4	11.4	Increased flexibility by specifying *intrusion-detection and/or intrusion prevention techniques to detect and/or prevent intrusions in the network* rather than "intrusion-detection systems and/or intrusion-prevention systems."	Clarification
11.5	11.5	Increased flexibility by specifying *change detection mechanism* rather than "file integrity monitoring."	Clarification
	11.5.1	New requirement to implement a process to respond to any alerts generated by the change-detection mechanism (supports 11.5)	Evolving Requirement
Requirement 12			
12.1.1 12.2	1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6	Combined former requirements at 12.1.1 (for the information security policy to address all PCI DSS requirements) and 12.2 (for operational security procedures), and moved them into Requirements 1 through 11, as a requirement in each.	Clarification
12.1.3	12.1.1	Moved former requirement 12.1.3 to 12.1.1.	Clarification
12.1.2	12.2	Moved former requirement 12.1.2 for an annual risk assessment process to 12.2, and clarified that the risk assessment should be performed at least annually *and after significant changes to the environment*.	Evolving Requirement
12.3.4	12.3.4	Clarified that "labeling" is an example of a method to be used.	Clarification
12.3.8	12.3.8	New testing procedure to verify policy is implemented for disconnecting remote access sessions after a specific period of inactivity.	Clarification
12.3.10	12.3.10	Aligned language between requirement and testing procedures to clarify that, where there is an authorized business need for personnel to access cardholder data via remote-access technologies, the data must be protected in accordance with all applicable PCI DSS Requirements.	Clarification
12.8	12.8	Clarified intent to implement and maintain policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.	Clarification

Requirement		Change	Type
PCI DSS v2.0	PCI DSS v3.0		
12.8.2	12.8.2	Clarified the applicable responsibilities for the service provider's written agreement/ acknowledgement.	Clarification
	12.8.5	New requirement to maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	Evolving Requirement
	12.9	New requirement for service providers to provide the written agreement/acknowledgment to their customers as specified at requirement 12.8. *Effective July 1, 2015*	Evolving Requirement
12.9.x	12.10.x	Renumbered requirement and updated 12.10.5 to clarify the intent is for alerts from *security monitoring systems* to be included in the incident response plan.	Clarification