PCi Security Standards Council®

Payment Card Industry (PCI)

Data Security Standard and Payment Application Data Security Standard

Version 3.0 Change Highlights

August 2013

Table of Contents

Introduction

This document from the PCI Security Standards Council (PCI SSC) highlights anticipated changes to the PCI Data Security Standard (PCI DSS) and Payment Application-Data Security Standard (PA-DSS) in order to prepare organizations for the introduction of Version 3.0 in November 2013. Its objectives are to:

- Help stakeholders prepare to review and discuss the draft versions of PCI DSS and PA-DSS at the 2013 Community Meetings.
- Prepare stakeholders to align their security programs with the updated Standards.
- Provide additional time for merchants to review and understand changes prior to implementation.

Publishing this document prior to release of more detailed information on the revised Standards is part of the PCI SSC's ongoing commitment to provide a steady flow of information during the standards development process and eliminate any perceived surprises in the process. With this in mind, please note this document is for advance informational purposes only and does not replace the current versions of PCI DSS and PA-DSS, the to-be-published detailed Summary of Changes, or Version 3.0 of the Standards.

The detailed Summary of Changes and draft versions of the Standards will be shared with Participating Organizations and the assessment community in early September, prior to discussion at the North American Community Meeting taking place in Las Vegas on 24-26 September.

Standards Development Lifecycle and Feedback Process

The PCI SSC develops security standards for the protection of payment card data in accordance with a defined 36-month lifecycle with eight stages, published on the Council's website.

As part of the open standards development process for the PCI DSS and PA-DSS, the PCI SSC solicits input on the Standards from its global stakeholders through a variety of avenues, including a formal feedback period. More than half the input received during the formal feedback period for Version 3.0 originated from organizations outside of the United States, with the majority specific to the PCI DSS. A full report of the feedback received is available on the PCI SSC website.

This industry feedback drives the ongoing development of strong technical standards for the protection of cardholder data, providing more than 700 Participating Organizations—including merchants, banks, processors, hardware and software developers, Board of Advisors, point-of-sale vendors, and the assessment community—the opportunity to play an active role in the improvement of global payment security.

Changes to PCI DSS and PA-DSS

Before introducing revisions to PCI DSS and PA-DSS the Council must weigh many considerations, including:

- What will improve payment security?
- Global applicability and local market concerns
- Appropriate sunset dates for other standards or requirements
- Cost/benefit of changes to infrastructure
- Cumulative impact of any changes

Based on feedback from the industry, in 2010 the Council moved from a two-year to a three-year standards development lifecycle. The additional year provides a longer period to gather feedback and more time for organizations to implement changes before a new version is released. Version 3.0 will introduce more changes than Version 2.0. The core 12 security areas remain the same, but the updates will include several new sub-requirements that did not exist previously. Recognizing that additional time may be necessary to implement some of these sub-requirements, the Council will introduce future implementation dates accordingly. This means until 1 July 2015 some of these sub-requirements will be best practices only, to allow organizations more flexibility in planning for and adapting to these changes. Additionally, while entities are encouraged to begin implementation of the new version of the Standards as soon as possible, to ensure adequate time for the transition, Version 2.0 will remain active until 31 December 2014.

The nature of the changes reflects the growing maturity of the payment security industry since the Council's formation in 2006, and the strength of the PCI Standards as a framework for protecting cardholder data. Cardholder data continues to be a target for criminals. Lack of education and awareness around payment security and poor implementation and maintenance of the PCI Standards leads to many of the security breaches happening today. The updates address these challenges by building in additional guidance and clarification on the intent of the requirements and ways to meet them. Additionally, the changes in PCI DSS and PA-DSS 3.0 focus on some of the most frequently seen threats and risks that precipitate incidents of cardholder-data compromise. The updated standards will help organizations not by making the requirements more prescriptive, but by adding more flexibility and guidance for integrating card security into their business-as-usual activities. At the same time, the changes will provide increased stringency for validating that these controls have been implemented properly, with more rigorous and specific testing procedures that clarify the level of validation the assessor is expected to perform. Overall, the changes are designed to give organizations a strong but flexible security architecture with principles that can be applied to their unique technology, payment, and business environments.

The updated versions of PCI DSS and PA-DSS will:

- Provide stronger focus on some of the greater risk areas in the threat environment
- Provide increased clarity on PCI DSS & PA-DSS requirements
- Build greater understanding on the intent of the requirements and how to apply them
- Improve flexibility for all entities implementing, assessing, and building to the Standards
- Drive more consistency among assessors
- Help manage evolving risks / threats
- Align with changes in industry best practices
- Clarify scoping and reporting
- Eliminate redundant sub-requirements and consolidate documentation

Change Drivers

The PCI Standards are updated based on feedback from the industry, per the standards development lifecycle as well as in response to current market needs. Common challenge areas and drivers for change include:

- Lack of education and awareness
- Weak passwords, authentication
- Third-party security challenges
- Slow self-detection, malware
- Inconsistency in assessments

Key Themes

Changes planned for Version 3.0 are designed to help organizations take a proactive approach to protect cardholder data that focuses on security, not compliance, and makes PCI DSS a business-as-usual practice. Key themes emphasized throughout Version 3.0 include:

- ### Education and awareness

  Lack of education and awareness around payment security, coupled with poor implementation and maintenance of the PCI Standards, gives rise to many of the security breaches happening today. Updates to the standards are geared towards helping organizations better understand the intent of requirements and how to properly implement and maintain controls across their business. Changes to PCI DSS and PA-DSS will help drive education and build awareness internally and with business partners and customers.

- ### Increased flexibility

  Changes in PCI DSS and PA-DSS 3.0 focus on some of the most frequently seen risks that lead to incidents of cardholder data compromise—such as weak passwords and authentication methods, malware, and poor self-detection—providing added flexibility on ways to meet the requirements. This will enable organizations to take a more customized approach to addressing and mitigating common risks and problem areas. At the same time, more rigorous testing procedures for validating proper implementation of requirements will help organizations drive and maintain controls across their business.

- ### Security as a shared responsibility

  Securing cardholder data is a shared responsibility. Today's payment environment has become ever more complex, creating multiple points of access to cardholder data. Changes introduced with PCI DSS and PA-DSS focus on helping organizations understand their entities' PCI DSS responsibilities when working with different business partners to ensure cardholder data security.

Emerging Technologies

PCI Standards provide a strong framework for protecting payment card data, regardless of the technology or platform used to accept or process it. The PCI DSS and PA-DSS are constructed in a way that their principles can be applied to various environments where cardholder data is processed, stored, or transmitted—such as e-commerce, mobile acceptance, or cloud computing. Specific guidance on the use of emerging technologies and how PCI Standards apply are currently addressed via information supplements produced by PCI Special Interest Groups, and separate guidance documents, such as *Mobile Payment Acceptance Security Guidelines for Merchants*. As the mobile environment develops, the Council will continue to work with industry stakeholders on developing relevant guidance and/or requirements as appropriate. Technologies such as point-to-point encryption and tokenization are being addressed as separate initiatives. For more information, please visit the PCI SSC website.

Change Highlights

Types of changes to the Standards are categorized as follows:

- **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.

The tables on the following pages provide insight into anticipated changes to the Standards, including the key feedback and market needs they aim to address.

PCI Data Security Standard (PCI DSS) 3.0

Note: *These proposed updates are still under review by the PCI community. Final changes will be determined after the PCI Community Meetings and incorporated into the final versions of the PCI DSS and PA-DSS published in November.*

Requirement	PCI DSS Update	Purpose / Need Addressed
1	Have a current diagram that shows cardholder data flows.	To clarify that documented cardholder data flows are an important component of network diagrams.
2	Maintain an inventory of system components in scope for PCI DSS.	To support effective scoping practices.
5	Evaluate evolving malware threats for systems not commonly affected by malware.	To promote ongoing awareness and due diligence to protect systems from malware.
6	Update list of common vulnerabilities in alignment with OWASP, NIST, SANS, etc., for inclusion in secure coding practices.	To keep current with emerging threats.
8	Security considerations for authentication mechanisms such as physical security tokens, smart cards, and certificates.	To address feedback that requirements for securing authentication methods other than passwords need to be included.
9	Protect POS terminals and devices from tampering or substitution.	To address need for physical security of payment terminals.
11	Implement a methodology for penetration testing, and perform penetration tests to verify that the segmentation methods are operational and effective.	To address requests for more details for penetration tests, and for more stringent scoping verification.
12	Maintain information about which PCI DSS requirements are managed by service providers and which are managed by the entity. Service providers to acknowledge responsibility for maintaining applicable PCI DSS requirements.	To address feedback from the Third Party Security Assurance SIG.

Requirement	PCI DSS Update	Purpose / Need Addressed
General	Clarified that sensitive authentication data must not be stored after authorization even if PAN is not present.	To ensure better understanding of protection of sensitive authentication data.
General	Added guidance for implementing security into business-as-usual (BAU) activities and best practices for maintaining on-going PCI DSS compliance.	To address compromises where the organization had been PCI DSS compliant but did not maintain that status. Recommendations focus on helping organizations take a proactive approach to protect cardholder data that focuses on security, not compliance, and makes PCI DSS a business-as-usual practice.
General	Added guidance for all requirements with content from the former *Navigating PCI DSS Guide*.	To assist understanding of security objectives and intent of each requirement.
General	ROC reporting section relocated to a separate reporting template.	To simplify and streamline the reporting process.
General	Enhanced testing procedures to clarify the level of validation expected for each requirement.	To put more emphasis on the quality and consistency of assessments.
Multiple	Incorporate security policy/procedure requirements into each requirement (replaces former 12.1.1 and 12.2).	To address feedback that policy topics should more closely align with the related technical PCI DSS requirement.
2	Clarified that changing default passwords is required for application/service accounts as well as user accounts.	To address gaps in basic password security practices that are leading to compromises.
3	Provided flexibility with more options for secure storage of cryptographic keys, and clarified principles of split knowledge and dual control.	To clarify common misunderstandings about key management.
8	Provided increased flexibility in password strength and complexity to allow for variations that are equivalent. Revised password policies to include guidance for users on choosing strong passwords, protecting their credentials, and changing passwords upon suspicion of compromise.	To address feedback on improving password security. Changes focus on increased flexibility and user guidance rather than new requirements.
10	Clarified the intent and scope of daily log reviews.	To help entities focus log-review efforts on identifying suspicious activity and allow flexibility for review of less-critical logs events, as defined by the entity's

Requirement	PCI DSS Update	Purpose / Need Addressed
		risk management strategy.

PCI Payment Application Data Security Standard (PA-DSS) 3.0

Note: *These proposed updates are still under review by the PCI community. Final changes will be determined after the PCI Community Meetings and incorporated into the final versions of the PCI DSS and PA-DSS published in November.*

Requirement	PA-DSS Update	Purpose / Need Addressed
5	Enhanced requirements for system development processes including periodic security reviews, verifying integrity of source code, a versioning methodology, use of application threat-modeling techniques, and a formal authorization process before final release.	To provide greater assurance regarding PA-DSS vendor development practices. This will allow for simplified processes for changes to PCI-listed applications and increased flexibility for vendors.
	For inclusion in secure coding practices, update list of common vulnerabilities in alignment with OWASP, NIST, SANS, etc.	To keep current with emerging threats.
7	New requirement for application vendor to provide release notes for all updates.	To help merchants more easily determine whether their application version is on the PA-DSS list.
14	New requirement to focus on training of integrators/resellers (formerly in Requirement 13) and vendor personnel.	To emphasize importance of training for integrator/reseller and vendor personnel.

Requirement	PA-DSS Update	Purpose / Need Addressed
General	Clarify that PA-DSS applications are in scope for an organization's PCI DSS assessment.	To address common misconception that use of a PA-DSS application guarantees PCI DSS compliance.
General	Added guidance for all requirements.	To assist understanding of security objectives and intent of each requirement.
General	Relocated ROV reporting section to a separate reporting template.	To simplify and streamline reporting process.
General	Relocated information on PA-DSS eligibility and roles and responsibilities to the PA-DSS Program Guide.	To provide more clarity by removing repetitive information.
General	Updated testing procedures for verifying contents of *PA-DSS Implementation Guides.*	To put more emphasis on quality Implementation Guides.
2	Removed requirement regarding use of full disk encryption solutions.	To address confusion on inclusion of this requirement in PA-DSS.
3	Enhanced requirements to ensure that changing of default passwords is enforced by the application and appropriately validated.	To address feedback that unchanged default passwords are a common cause of merchant compromises.
	Updated requirement to require use of a one-way cryptographic algorithm with an input variable to render passwords unreadable.	To address feedback that passwords need to be stored and transmitted more securely.
8	Relocated two requirements from Requirement 5 and 10 to align them with other requirements that facilitate a secure PCI DSS environment.	To clarify intent of the requirements for improved understanding.
10	Clarified the requirement for two-factor authentication applies to network access originating outside the customer's network.	To improve understanding of when two-factor authentication is applicable.
13	Refocused requirement solely on the Implementation Guide, and removed requirements for training of integrators/resellers to new Requirement 14.	To put more emphasis on quality Implementation Guides.

Conclusion

The PCI Security Standards Council thanks the hundreds of companies and stakeholders that have taken the time to provide us with feedback on the PCI Security Standards. This valuable, real-world input ensures that the Standards can continue to provide a strong security framework for the protection of cardholder data.

The Council looks forward to welcoming stakeholders to our annual Community Meetings and discussing the detailed Summary of Changes and draft versions of the Standards, which will be provided to Participating Organizations and the assessment community in early September.

This document provides insight into anticipated changes to the PCI DSS and PA-DSS for advance informational purposes only, and does not replace the current standards, the to-be-published detailed Summary of Changes or new versions of the Standards. The planned publication date of Versions 3.0 of PCI DSS and PA-DSS is 7 November 2013, after they have been discussed at the Council's European Community Meeting in Nice. The updated Standards will become effective on 1 January 2014, per the lifecycle. Entities are encouraged to begin implementation of the new version of the Standards as soon as possible; but to ensure adequate time for the transition, Version 2.0 will remain active until 31 December 2014.