PCI DSS 2.0 and PA-DSS 2.0 SUMMARY OF CHANGES - HIGHLIGHTS

Introduction

This document from the PCI Security Standards Council (PCI SSC) is designed to provide a transparent runway to the introduction of the new versions of PCI Data Security Standard (PCI DSS) and Payment Application-Data Security Standard (PA-DSS) targeted for release at the end of October. The purpose of the document is to share highlights of forthcoming changes to the standards in order to:

- Help stakeholders prepare to review and discuss the new pre-release versions of PCI DSS and PA-DSS at forthcoming Community Meetings in the US and Europe
- Prepare stakeholders to align their security programs with the updated standards
- Provide additional time for merchants to review and understand changes prior to implementation

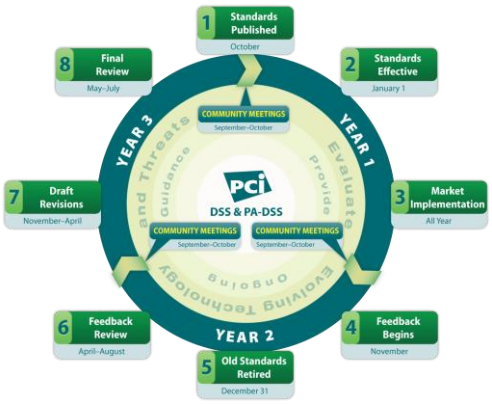
Publishing this document prior to release of more detailed information on the revised standards is part of the PCI SSC's ongoing commitment to providing a steady flow of information during the standards development process and eliminating any perceived surprises in the process. With that in mind, the SSC asks stakeholders to understand that the detailed summary of changes and pre-release versions of the standards will be shared with Participating Organizations in early September, prior to the North American Community Meeting taking place in Orlando on Sept 21-23. We hope Participating Organizations will join us at the Community Meeting to discuss the updates in more depth. Please note this document is for advance informational purposes only, and does not replace the current DSS, the to-be-published detailed summary of changes or new versions of the standards.

The Standards Development Lifecycle and Feedback Process

The PCI Security Standards Council develops security standards for the protection of payment card data in accordance with a planned lifecycle which is published on our website. The lifecycle ensures multiple opportunities for stakeholder input and feedback on standards, which is a vital part of ensuring PCI Security Standards remain ahead of the threat landscape. In June the SSC announced that in response to stakeholder feedback, the lifecycle for development of PCI Security Standards would move to a three year cycle from the previous two year cycle. This additional year provides extra opportunities for stakeholder input and feedback, a longer time period for the feedback to be submitted and more merchant friendly start date to implement, along with longer sunset periods for existing standards. Now all three PCI Standards (PCI DSS, PA-DSS and PTS requirements) operate on a three year lifecycle. For more information on the new lifecycle please see the following factsheets on the PCI SSC website:
https://www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf

https://www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_pts.pdf

The new three year lifecycle becomes effective on publication of the revised PCI DSS and PA-DSS standards at the end of October.



During the current revision cycle the SSC received hundreds of pieces of feedback from stakeholders around the world through the lifecycle feedback form. In addition to this formally submitted feedback the Council gathers comments through our Open Mic series, the Community Meeting discussions, input from Special Interest Groups, online FAQ portal and other industry events. In this feedback cycle more than half of the feedback submitted originated outside of the United States.

Upcoming Changes to PCI DSS and PA-DSS

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

- What is best for 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

Stakeholders will notice that the changes to PCI DSS 2.0 and PA-DSS 2.0 are relatively straightforward and do not introduce significant changes. This reflects the growing maturity of the standards as a strong framework for protecting cardholder data. The updated versions of PCI DSS and PA-DSS will:

- Provide greater clarity on PCI DSS & PA-DSS requirements
- Improve flexibility for merchants
- Help manage evolving risks / threats
- Align with changes in industry best practices

- Clarify scoping and reporting
- Eliminate redundant sub-requirements and consolidate documentation

Feedback gathered during the current cycle led to suggested changes that naturally fell into three main categories of change:

- Clarification: Modification that clarifies intent of requirement; ensures that concise wording in the standards portray the desired intent of requirements
- Additional Guidance: Provides further information on a particular topic to increase understanding of the intent of the requirement
- Evolving Requirement: Requirement outlining situation not addressed in a standard; ensures the standards are up-to-date with emerging threats and changes in the market

The following highlight table provides insight into the areas of feedback and changes anticipated and where they fall in these categories.

Requirement Impact	Reason for Change	Proposed Change	Category
PCI DSS Intro	Clarify Applicability of PCI DSS and cardholder data.	Clarify that PCI DSS Requirements 3.3 and 3.4 apply only to PAN. Align language with PTS Secure Reading and Exchange of Data (SRED) module.	Clarification
Scope of Assessment	Ensure all locations of cardholder data are included in scope of PCI DSS assessments	Clarify that all locations and flows of cardholder data should be identified and documented to ensure accurate scoping of cardholder data environment.	Additional Guidance
PCI DSS Intro and various requirements	Provide guidance on virtualization.	Expanded definition of system components to include virtual components. Updated requirement 2.2.1 to clarify intent of “one primary function per server” and use of virtualization.	Additional Guidance
PCI DSS Requirement 1	Further clarification of the DMZ.	Provide clarification on secure boundaries between internet and card holder data environment.	Clarification
PCI DSS Requirement 3.2	Clarify applicability of PCI DSS to Issuers or Issuer Processors.	Recognize that Issuers have a legitimate business need to store Sensitive Authentication Data.	Clarification

Requirement Impact	Reason for Change	Proposed Change	Category
PCI DSS Requirement 3.6	Clarify key management processes.	Clarify processes and increase flexibility for cryptographic key changes, retired or replaced keys, and use of split control and dual knowledge.	Clarification
PCI DSS Requirement 6.2	Apply a risk based approach for addressing vulnerabilities.	Update requirement to allow vulnerabilities to be ranked and prioritized according to risk.	Evolving Requirement
PCI DSS Requirement 6.5	Merge requirements to eliminate redundancy and Expand examples of secure coding standards to include more than OWASP.	Merge requirement 6.3.1 into 6.5 to eliminate redundancy for secure coding for internal and Web-facing applications. Include examples of additional secure coding standards, such as CWE and CERT.	Clarification
PCI DSS Requirement 12.3.10	Clarify remote copy, move, and storage of CHD.	Update requirement to allow business justification for copy, move, and storage of CHD during remote access.	Clarification
PA DSS General	Payment Applications on Hardware Terminals.	Provide further guidance on PA-DSS applicability to hardware terminals.	Additional Guidance
PA-DSS Requirement 4.4	Payment applications should facilitate centralized logging.	Add sub-requirement for payment applications to support centralized logging, in alignment with PCI DSS requirement 10.5.3.	Evolving Requirement
PA-DSS Requirements 10 & 11	Merge PA-DSS Requirements 10 and 11	Combine requirements 10 and 11 (remote update and access requirements) to remove redundancies.	Clarification

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 in Orlando and Barcelona and discussing the more detailed summary of changes and pre-release versions of the revised standards, which will be provided to Participating Organizations in early September. As a reminder, 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 DSS, the to-be-published detailed summary of changes or new versions of the standards. The planned publication date of versions 2.0 of PCI DSS and PA-DSS is October 28, 2010, after they

have been discussed at the Council's European Community Meeting in Barcelona. Per the new three year lifecycle, the updated standards will become effective on January 1, 2011.