Feedback Highlights

Examples of Input Shared with the PCI Security Standards Council during the PCI Standards Feedback Period

June 2010

Overview

The Payment Card Industry Security Standards Council manages technical standards used to secure cardholder data that is stored, processed, or transmitted by merchants, financial institutions and other organizations. Three standards govern this objective: the PCI Data Security Standard (PCI DSS), the Payment-Application Data Security Standard (PA-DSS), and the PIN Transaction Security (PTS) requirements. All three standards follow a defined lifecycle to ensure a gradual, phased introduction of revisions to the standards in order to prevent organizations from becoming noncompliant when changes are published. .Input for changes to these standards comes from many worldwide sources and is gathered through formal and informal channels including the PCI Standards lifecycle feedback form, intelligence garnered from the assessment community and feedback from questions asked by stakeholders online and at industry events. Suggestions for proposed changes are also made by Participating Organizations globally, which include merchants, banks, processors, hardware and software developers, point-of-sale vendors, as well as the assessment community consisting of Qualified Security Assessors and Approved Scanning Vendors. Contributions to standards development is also made by the PCI SCC founders – American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. In 2010 close to 400 PCI Standards lifecycle feedback forms were submitted, each containing up to 5 pieces of feedback. Over 50% of feedback submitted came from organizations based outside of the United States, a strong indication of the standards' global utility as well as recognition of the need for a unified, worldwide response to combat the global threat of payment card fraud.

The Council solicits such broad, global feedback to ensure that the standards meet evolving risks and threats, and align with changes in industry best practices. Feedback typically falls under any of three categories:

Clarifications –Feedback categorized as "clarification" identifies wording in standards that may be potentially be perceived as confusing or cumbersome. The goal of addressing clarification feedback is to ensure that concise wording is utilized in the standards to portray the desired intent of requirements. Some examples of resulting changes based on clarification feedback include generally minor wording changes, test procedure alignments, or glossary definition updates.

Additional Guidance –The "additional guidance" category is utilized to categorize any feedback that identifies a need for further detail in understanding the intent of a requirement. The goal of addressing additional guidance feedback is to provide further information on a particular

topic that would not be suitable to include directly into a particular example. Additional Guidance is generally provided via FAQs, Information Supplements, or the DSS Navigation Guide.

Evolving Requirements – "Evolving Requirements" are noted based on feedback that outlines a particular situation not addressed in a standard. The goal of addressing evolving requirements feedback is to ensure that the standards are up to date with emerging threats and changes in the market. Examples of evolving requirements may include modifying the wording of a requirement to change the intent and, on rare occasion, the introduction of a new requirement.

In addition to the submitted PCI Standards lifecycle feedback form, over the course of each development lifecycle the SSC receives thousands of pieces of feedback through channels such as webinar questions, training attendee input, Community Meeting discussion, assessor meetings and interactions, "@info" and "askbob" email aliases. Common themes in feedback are regularly addressed through the SSC's online Frequently Asked Questions tool, which provides a venue for the SSC to provide the latest guidance to the market. On a particular issue, comments often address multiple and even contradictory perspectives, so a summary is difficult without including numerous examples and commentary. The examples below are intended to provide a window into commentary received by the Council rather than a complete executive summary of all feedback. While these examples cite specific requirements in the standards, they do not necessarily preview changes that will occur in future versions.

Clarifications

Example 1 – Articulating a Technical Concept

Some Participating Organizations desire more clarity in the definition of key technical concepts associated with the standards. One example is the Demilitarized Zone (DMZ), which may play an important role in segmenting a secure boundary between the internet and a cardholder data environment. Clarification of the DMZ would be an added component of PCI DSS Requirement 1, which addresses the use of firewalls and routers for protecting cardholder data.

Example 2 – Addressing Inconsistency

PCI standards apply to multiple constituencies, which may not always share the same operational requirements. For this reason, specific points may require clarification. For example, PCI DSS Requirement 3.2 has almost become a mantra: *Do not store sensitive authentication data after authorization (even if it is encrypted)*. This statement is universally true for merchants, but its applicability may be different for some Issuers or Issuer Processors. Clarification would provide new guidance around Issuer scenarios and best practices.

Example 3 – Addressing Vague Terminology

The wording of some provisions in the standards may be subject to different interpretations. For example, some Participating Organizations have requested more specificity in clarifying minimum requirements for rendering cardholder data unreadable. PCI DSS Requirement 3.4 lists five candidate solutions for this objective. Clarification would articulate examples of acceptable versus unacceptable implementations of these technologies.

Additional Guidance

Example 1 – Updating Documentation for Validation

With the evolution of technology, it is important to update PCI validation paperwork to reflect solutions that are deployed in production environments. One example is Self-Assessment Questionnaires (SAQs), which could list all common technology pertinent to self-evaluation by a merchant.

Example 2 – Addressing New Technology

The card payment environment is constantly exposed to use of new technology. It is important for the standards to address these, especially if the new technology is in prevalent deployment and affects multiple requirements. One example of a new technology fitting this description is virtualization.

Evolving Requirements

Example 1 – Retiring Old Technology

Some security solutions outlive their utility. For example, encryption is a mature technology, but encryption key lengths that used to be strong are now weak and have been replaced by longer, more robust key lengths. This topic is germane to PCI DSS Requirements 2.1.1, 3.4, 4 and elsewhere. Practically addressing questions about this topic may entail associating sunset dates with old technology to ensure that an organization has actually deployed strong cryptography.

Example 2 – Addressing Complexity

As Participating Organizations gain more experience with the standards, some are looking for a deeper treatment of risks that have grown in complexity. For example, PCI DSS Requirement 6.5 directs organizations to develop all Web applications based on secure coding guidelines and review custom application code to identify coding vulnerabilities. Enhancing guidance for this requirement could include specifying multiple frameworks or standards that address the complexity of creating comprehensive security for application code.

Example 3 – Expanding Certification

Participating Organizations seek assurance that the hardware and software deployed in a cardholder data environment are secure, and whenever possible, are certified for use by the standards. One newer solution falls under the moniker of “End-to-End Encryption” (E2EE) or the term used by the Council, point-to-point encryption. Some implementations of point-to-point encryption would have encryption

occur in the Hardware Terminal; decryption would only be possible by the Acquirer/Processor. Participating Organizations wishing to deploy such a solution would seek the ability for payment applications on Hardware Terminals to be certified under PA-DSS, which would necessitate a corresponding change to that standard.

Summary

The PCI Security Standards Council appreciates the collaborative effort of Participating Organizations, Council founders and industry stakeholders to make its standards for securing cardholder data strong and effective. The Council has carefully analyzed all feedback provided for current versions of the PCI standards and is incorporating that information in revisions to be published in October 2010. It is important to reiterate that the examples given above are for the purpose of providing a window into the feedback process, rather than any value judgement on specific feedback topics or a preview to forthcoming revisions to the standards. With effective, up-to-date PCI standards and any corresponding guidance materials, Participating Organizations worldwide have the ability to implement and maintain a layered approach to security that keeps cardholder data secure.