



Security
Standards Council

Prioritized Approach for PCI DSS 1.2

Bob Russo, general manager PCI SSC
Jennifer Mack, PCI SSC Marketing Working Group chair

- Introductions
- New resource – Prioritized Approach
- Standards Training
- Q&A

What is it?

- Guidance for organizations to prioritize their PCI DSS implementation efforts

What are the benefits?

- Provides a roadmap that an organization can use to address risks in priority order
- Enables merchants, of any size, to demonstrate progress on PCI DSS compliance process to key stakeholders – banks, acquirers, QSAs and others
- Promotes objective and measurable progress indicators

How was it created?

- Payment brands' examination of account data compromise events
- Feedback from PCI SSC Board of Advisors, Council leadership and the Technical Working Group
- Feedback from several QSAs and forensics investigators
 - Asked to identify the top 15 PCI DSS requirements for protecting cardholder data



Objectives of Prioritized Approach

- Prioritize efforts based on the risk associated with handling cardholder data
 - Security efforts can first focus on certain PCI DSS requirements
- Reduce risk associated with account data compromise by:
 - Not retaining magnetic stripe data
 - Minimize and secure storage of PAN
 - Using network segmentation to reduce scope



The Prioritized Approach can

- Help merchants know where to start with PCI DSS compliance
- Prompt merchants to consider a risk based approach when evaluating their PCI DSS implementation timelines and budgets
- Facilitate discussion between a merchant and stakeholders on progress with PCI DSS



The Prioritized Approach does not

- Provide a short cut to compliance with PCI DSS 1.2
- Assume a one size fits all approach for every organization
- Replace PCI DSS 1.2



Prioritized Approach Tools

Reference Guide

PCI COMPLIANCE IS A CONTINUOUS PROCESS



Disclaimer

To achieve PCI DSS compliance, an organization must meet all PCI DSS requirements, regardless of the order in which they are satisfied or whether the organization seeking compliance follows the PCI DSS Prioritized Approach. This document does not modify or abridge the PCI DSS or any of its requirements, and may be changed without notice. PCI SSC is not responsible for errors or damages of any kind resulting from the use of the information contained herein. PCI SSC makes no warranty, guarantee, or representation as to the accuracy or sufficiency of the information provided herein, and assumes no responsibility or liability regarding the use or misuse of such information.

Milestones for Prioritizing PCI DSS Compliance Efforts

The Prioritized Approach includes six milestones. The matrix below summarizes high-level goals and intentions of each milestone. The rest of this document details milestones to each of all twelve PCI DSS requirements and their sub-requirements.

PCI SSC FOUNDERS



PARTICIPATING ORGANIZATIONS

Merchants, banks, processors, developers and point of sale vendors

| Milestone | Goals |
|-----------|---|
| 1 | Remove sensitive authentication data and limit data retention. This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are stored, the effects of a compromise will be greatly reduced. If you don't store it, you can't compromise it. |
| 2 | Protect the perimeter, internal, and wireless networks. This milestone targets controls for points of access to most compromises – the wireless access point. |
| 3 | Secure payment card applications. This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining cardholder data. |
| 4 | Monitor and control access to your systems. Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment. |
| 5 | Protect stored cardholder data. For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data. |
| 6 | Finalize all policies, procedures, and processes to support maintenance of PCI DSS compliance. The intent of Milestone 6 is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment. The milestone also includes completion of firewall configuration standards, change control procedures, securing audit trails, and network testing processes. |

| PCI DSS Requirements | Milestone | | | | | |
|--|-----------|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| Requirement 1: Install and maintain a firewall configuration to protect cardholder data | | | | | | |
| 1.1 Establish firewall and router configuration standards that include the following: | | | | | | 6 |
| 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations | | | | | | |
| 1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks | 1 | | | | | |
| 1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone | | 2 | | | | |
| 1.1.4 Description of groups, roles, and responsibilities for logical management of network components | | | | | | 6 |
| 1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure | | 2 | | | | |
| 1.1.6 Requirement to review firewall and router rule sets at least every six months | | | | | | 6 |
| 1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment. | | 2 | | | | |
| 1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. | | | | | | |

Prioritized Approach Tools

Worksheet & Attestation of Compliance

| PCI DSS Requirements Version 1.2 | Milestone | Status: <i>Please enter "yes" if fully compliant with the requirement</i> | Comments |
|--|-----------|--|----------|
| Requirement 1: Install and maintain a firewall configuration to protect cardholder data. | | | |
| 1.1 Establish firewall and router configuration standards that include the following: 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations | 6 | | |
| 1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks | 1 | | |
| 1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone | 2 | | |
| 1.1.4 Description of groups, roles, and responsibilities for logical management of network components | 6 | | |
| 1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure | 2 | | |
| 1.1.6 Requirement to review firewall and router rule sets at least every six months | 6 | | |
| 1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment. 1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. | 2 | | |
| 1.2.2 Secure and synchronize router configuration files. | 2 | | |
| 1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. | 2 | | |
| 1.3 Prohibit direct public access between the Internet and any system components in the cardholder data environment. | 2 | | |

Prioritized Approach Summary & Attestation of Compliance

| Milestone | Goal | Percent Complete | Estimated Date for Completion of |
|-----------|---|------------------|----------------------------------|
| 1 | Remove sensitive authentication data and limit data retention. This milestone targets a key area of risk for entities that have been compromised. Remember - if sensitive authentication data and other cardholder data are not stored, the impact of a | 0.0% | |
| 2 | Protect the perimeter, internal, and wireless networks. This milestone targets controls for points of access to most compromised - the network or wireless access point. | 0.0% | |
| 3 | Secure payment card applications. This milestone targets controls for applications, application processor, and application servers. Weaknesses in these areas offer a very easy way for some criminals to obtain access to | 0.0% | |
| 4 | Monitor and control access to your systems. Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment. | 0.0% | |
| 5 | Protect stored cardholder data. For those organizations that have analyzed their business processor and determined that they maintain Primary Account Numbers, Milestone Five targets key protection mechanisms for that | 0.0% | |
| 6 | Finalize remaining compliance efforts, and ensure all controls are in place. The intent of Milestone Six is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data | 0.0% | |
| Overall | | 0.0% | |

We hereby attesting this summary to comply with the PCI DSS. We will keep copies of the prepared controls, and all prepared controls require this attestation.

Part 5: Target Date for Achieving Full PCI DSS Compliance _____ Date _____

Part 6: Merchant or Service Provider Acknowledgements

Executive Officer _____ Date _____

Six Security Milestones



Milestone One - If you don't need it, don't store it.

The intent of Milestone One is to remove sensitive authentication data and limit data retention. This milestone targets a key area of risk for entities that have been compromised – if sensitive authentication data and other cardholder data had not been stored, the effects of the compromise would have been greatly reduced.

Milestone Two - Secure the perimeter.

The intent of Milestone Two is to protect the perimeter, internal, and wireless networks. This milestone targets a key area that represents the point of access for most compromises: vulnerabilities in networks or at wireless access points.

Milestone Three - Secure applications.

The intent of Milestone Three is to secure applications. This milestone focuses on applications, as well as application processes and application servers, since application weaknesses are a key access point used to compromise systems and obtain access to cardholder data.

Milestone Four - Control access to your systems.

The intent of Milestone Four is to protect the cardholder data environment through monitoring and access control since this is the key method to detect the who, what, when and how about who is accessing your network.

Milestone Five - Protect stored cardholder data.

For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data.

Milestone Six - Finalize remaining compliance efforts, and ensure all controls are in place.

The intent of Milestone Six is to complete PCI DSS requirements and finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

Important Note and Disclaimer

- In order to achieve PCI DSS compliance, ALL PCI DSS requirements must be successfully implemented, regardless of the order in which they are satisfied or whether the organization seeking compliance follows the PCI DSS Prioritized Approach. The Prioritized Approach does not, and is not intended in any manner to, modify or abridge the PCI DSS or any of its requirements.
- All information published by PCI SSC for the Prioritized Approach is subject to change without notice. PCI SSC is not responsible for errors or damages of any kind resulting from the use of the information contained therein. PCI SSC makes no warranty, guarantee, or representation as to the accuracy or sufficiency of the information provided as part of the Prioritized Approach, and PCI SSC assumes no responsibility or liability regarding the use or misuse of such information.

First PCI SSC Standards Training *Merchant training offered directly by PCI SSC*

- **Objective:** Arm merchants with everything they need to know to best prepare for an onsite PCI DSS assessment or to perform the assessment internally
- **Focus:** Four key modules
 - PCI Program – defining the payment card industry
 - Scoping a PCI DSS Assessment
 - PCI DSS v1.2 Requirements
 - Compensating Controls
- **Where:** Chicago on April 6-7, 2009
 - Check PCI SSC Website for additional locations and dates



PCI Security Standards Council
Standards Training Program 2009

A comprehensive PCI Standards Training program endorsed by the PCI SSC

The Payment Card Industry Security Standards Council (PCI SSC) is pleased to announce the first PCI SSC sponsored Standards Training Session taking place April 6-7, 2009 in Chicago, IL.

This is a 2-day training course based directly on the PCI SSC Qualified Security Assessor (QSA) training program. Attendees will learn what the QSA's learn so they can better prepare for an on-site PCI DSS assessment or perform the assessment internally.

| | | | |
|---------------------------------|----------------------------------|---|--|
| Date: April 6-7, 2009 | Time: 8:30am to 5:00pm | Location: University of Chicago Gleacher Center 450 North Clayfont Plaza Drive Chicago, IL 60611 US | Cost: \$995 US for 2-day training session |
|---------------------------------|----------------------------------|---|--|

For more information and to register please go to:
<https://www.pcisecuritystandards.org/education/training.shtml>

 Space is limited so please register today!
If you have any questions about this training, please contact
April Turcotte at aturcotte@pcisecuritystandards.org.

Question & Answer Session

