PCI Compliance
2012 - The Road Ahead
October 2012
Hari Shah & Parthiv Sheth
Point-to-Point Encryption (P2PE) Program Guide

Updated Solution Requirements and Testing Procedures for hardware-based P2PE solutions.
Provide a method for vendors to validate their P2PE solutions and for merchants to reduce the scope of their PCI DSS assessments by using a validated P2PE solution for accepting and processing payment card data.

Mobile Payment Acceptance Security

A fact sheet provides merchants with actionable recommendations on partnering with a Point-to-Point Encryption (P2PE) solution provider to securely accept payments and meet their PCI DSS compliance obligations.

PCI Mobile Payment Acceptance Security Guidelines

Offers software developers and mobile device manufacturers guidance on designing appropriate security controls to provide solutions for merchants to accept mobile payments securely.
Recent Updates to PCI Compliance Standard

- **ATM Security Guidelines Information Supplement (Draft)**
  
  Draft information supplement provides best practices to mitigate the effect of attacks to ATMs aimed at stealing PIN and account data, a direct response to stakeholder feedback for guidance on ATM security.

- **Qualified Integrators and Resellers (QIR) Program**
  
  New PCI SSC program will train and qualify integrators and resellers that sell, install and/or service payment applications on the secure installation and maintenance of PA-DSS validated payment applications to support merchant PCI DSS security efforts.

- **2013 Special Interest Group (SIG) Projects**
  
  Leverage the expertise of more than 600 Participating Organizations and assessors and provide a vehicle for incorporating their ideas and input into the work of the Council.

   *(Cloud, eCommerce and Risk Assessment)*
Feedback on v2.0

Updates to be considered for next release – October 2013

- **Scope of Assessment**
  Suggestions for detailed guidance on scoping and segmentation.

- **Requirement 3.4** - Render PAN unreadable
  Suggestions for further clarification and guidance since encryption and key management are complex requirements, and truncation/hashing & tokenization is not a convenient method to store and retrieve data.

- **Requirement 8.5** - User identification & authentication management for non-consumer users and administrators
  Suggestions for updating password requirements, including expanding authentication beyond just passwords; current password requirements are either too strict or not strict enough, be either less prescriptive or more prescriptive.
Updates to be considered for next release – October 2013

- **Requirement 11.2** - Internal and external network vulnerability scans
  
  Suggestions include prescribing use of specific tools, requiring ASVs to perform internal scans, and defining what constitutes a “significant change”.

- **Requirement 12.8** - Manage service providers
  
  Suggestions include clarifying the terms “service provider” and “shared,” and providing more prescriptive requirements regarding written agreements that apply to service providers.

- **PCI DSS SAQs** – Self-Assessment Questionnaires
  
  Suggestions for updating the SAQs; they are either too complex or not detailed enough.
The Reality
Current Compliance Challenges

Are you really 100% compliant?

- Assessor’s focus varies each year – gotta find something new!
- Raising the bar on QSAs reporting requirements
- The standard or requirement just changed
- Each entity and QSA have their own interpretation
- New policies or processes not fully implemented yet
- New projects or changes implemented without InfoSec review
### External User – Use Case

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Estimated Population Size</th>
<th>Estimated % of Visa Transactions</th>
<th>PCI DSS Compliance Validation</th>
<th>Validated Not Storing Prohibited Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1 Merchant (&gt;6M)</td>
<td>403</td>
<td>50%</td>
<td>97%</td>
<td>100%</td>
</tr>
<tr>
<td>Level 2 Merchant (1-6M)</td>
<td>1058</td>
<td>13%</td>
<td>93%</td>
<td>100%</td>
</tr>
<tr>
<td>Level 3 Merchant (e-commerce only 20,000 – 1M)</td>
<td>3,218</td>
<td>&lt; 5%</td>
<td>60%</td>
<td>N/A</td>
</tr>
<tr>
<td>Level 4 Merchant (&lt;1M)</td>
<td>~ 5,000,000</td>
<td>32%</td>
<td>Moderate**</td>
<td>TBD</td>
</tr>
</tbody>
</table>

*As of June 30, 2012

**Level 4 compliance is moderate among stand-alone terminal merchants, but lower among merchants using integrated payment applications
Common Failures

- Scoping Gaps
- Encryption Key Management
- Lack of adequate/required documentation
- Unnecessary Card Holder Data Storage
- Third-Party Compliance
- Internal & External Applications (PA-DSS & Req. 6.x)
- Comprehensive Monitoring & Logging
- Rogue Wireless
- Vulnerability Remediation
- Compensating Controls
Upcoming Compliance Challenges

- Mobile Devices – In-Stores & Corporate
- End-to-End Encryption & Tokenization
- Mobile Wallet
- Protecting Endpoints - Malware & White-Listing
- Social Network Integration
The Auditor’s Role
Approaching PCI

Potential Role of Internal Audit

Usually in an organization there is a single point ownership for PCI compliance. This can be the CIO, CISO or the Internal Audit department.

Here are some of the benefits of having an Internal Audit department own the compliance efforts:

- PCI DSS is somewhat similar in approach to SOX. Internal Auditors are close to internal policies and procedures and can easily supplement or lead compliance efforts. And with the right skills, IT auditors can now assess and report on compliance for level 1 merchants.

- Provide an independent assurance to the Board and Senior Management on compliance efforts.

- Effective and efficient than having external parties perform the audit.
Certification Programs

PCI SSC Internal Security Assessor (ISA)

- A certification program for individuals from large merchants, acquiring banks and processors who wants to build expertise in PCI standards and assessment
- Intended for individuals who already possess significant security audit and assessment expertise
- Requires company sponsorship and is non-transferable
- Qualification requirements include minimum five years work experience including one year performing security assessments, strong knowledge of PCI and related areas and one of the following industry recognized certifications – CISSP, CISA or CISM or relevant work experience
Certification Programs

Payment Card Industry Professional (PCIP)

- A certification program for individuals who want to demonstrate their knowledge of PCI standards and requirements

- Certification belongs to the individual and is not associated with the sponsoring organization

- Qualification requirements include minimum two years work experience in IT or IT related role

- Provides a starting point for entry-level and seasoned professionals and consultants to launch a career in the payment card industry
## Audit Approach

<table>
<thead>
<tr>
<th>For Level 1 Merchants</th>
<th>For Level 2, 3 and 4 Merchants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a top-down approach to identify all the points where credit card data flows across the organization</td>
<td>Participate in scoping exercise</td>
</tr>
<tr>
<td>Identify policies, procedures and controls in place to address the risk of a data breach and/or theft</td>
<td>Internal auditors can lead the Self Assessment Questionnaire process</td>
</tr>
<tr>
<td>Benchmark with the PCI DSS requirements to perform a gap analysis</td>
<td></td>
</tr>
<tr>
<td>Follow the PCI DSS Security Audit Procedures to test the requirements</td>
<td>IA can issue an independent report to the Board on the effectiveness of the PCI program</td>
</tr>
<tr>
<td>Work with the acquiring back to issue a report on compliance</td>
<td>Suggest compensating controls and help prioritize remediation efforts</td>
</tr>
<tr>
<td>Work with the control owners to assess risk, prioritize and remediation gaps</td>
<td></td>
</tr>
</tbody>
</table>

## Sustain Compliance

- Annual Risk Assessment
- On-going Audits
Summary of Changes (136)

[Imported Content]

- **Clarifications**
  - 119 total
  - Wording portrays intent

- **Additional Guidance**
  - 15 total
  - Increase understanding

- **Evolving Requirements**
  - 2 total
  - Emerging threats and changes

Source: