AGENDA

1. PCI SSC Standards Development
2. Current Standards Lifecycle
3. New Three Year Standards Lifecycle
4. PCI SSC Resources
PCI Security Standards Development
• Open, global forum
• Founded 2006
• Responsible for PCI Security Standards
  – Development
  – Management
  – Education
  – Awareness
PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data

MANUFACTURERS
PCI PTS
PIN Transaction Security Devices

SOFTWARE DEVELOPERS
PCI PA-DSS
Payment Application Vendors

MERCHANTS & PROCESSORS
PCI DSS
Data Security Standard

PCI SECURITY STANDARDS & COMPLIANCE

Ecosystem of payment devices, applications, infrastructure and users
Current PCI Standards Lifecycle

1. Market Implementation (10/1/08–6/30/09)
2. Feedback Begins (7/1/09–10/31/09)
3. Feedback Review and Decision (11/1/09–4/30/10)
5. Discuss New Version / Revision (9/30/10)
Move to Three Year Lifecycle

1. Market Implementation (10/1/08 – 6/30/09)
2. Feedback Begins (7/1/09 – 10/31/09)
3. Feedback Review and Decision (11/1/09 – 4/30/10)
5. Discuss New Version / Revision (9/30/10)

YEAR 1
1. Standards Published
   - October
2. Standards Effective
   - January 1
3. Market Implementation
   - All Year

YEAR 2
4. Feedback Begins
   - November
5. Old Standards Retired
   - December 31
6. Feedback Review
   - April-August
7. Draft Revisions
   - November-April
8. Final Review
   - May-July

YEAR 3
3. COMMUNITY MEETINGS
   - September-October
4. COMMUNITY MEETINGS
   - September-October
5. COMMUNITY MEETINGS
   - September-October
6. COMMUNITY MEETINGS
   - September-October

Evolving Technology
DSS & PA-DSS
Three Year Lifecycle
Lifecycle for Changes to PCI DSS and PA-DSS

1. Standards Published
   - October

2. Standards Effective
   - January 1

3. Market Implementation
   - All Year

4. Feedback Begins
   - November

5. Old Standards Retired
   - December 31

6. Feedback Review
   - April–August

7. Draft Revisions
   - November–April

8. Final Review
   - May–July

COMMUNITY MEETINGS
- September–October

Evolving Technology

Organizations

Provide Guidance

and Threats

YEAR 3

YEAR 2

YEAR 1
Stage 1 – Standards Published
Stage 2 – Standards Effective

1. Standards Published
   - October

2. Standards Effective
   - January 1

YEAR 3
- COMMUNITY MEETINGS
  - September–October

YEAR 1
- Market Implementation
  - All Year

YEAR 2
- Feedback Review
  - April–August
- Old Standards Retired
  - December 31

YEAR 3
- Draft Revisions
  - November–April
- COMMUNITY MEETINGS
  - September–October

Final Review
- May–July
Stage 3 – Market Implementation

1. Standards Published
   - October
2. Standards Effective
   - January 1
3. Market Implementation
   - All Year
4. Feedback Begins
   - November
5. Old Standards Retired
   - December 31
6. Feedback Review
   - April–August
7. Draft Revisions
   - November–April
8. Final Review
   - May–July
Stage 4 – Feedback Begins

1. Standards Published
   October

2. Standards Effective
   January 1

3. Market Implementation
   All Year

4. Feedback Begins
   November

5. Old Standards Retired
   December 31

6. Feedback Review
   April–August

7. Draft Revisions
   November–April

8. Final Review
   May–July

YEAR 1
- Evaluate
- Provide
- Evolving Technology

YEAR 2
- DSS & PA-DSS
- Guidance
- and Threats

YEAR 3
- COMMUNITY MEETINGS
  September–October

COMMUNITY MEETINGS
  September–October

COMMUNITY MEETINGS
  September–October

PCI Security Standards Council
Stage 5 – Old Standards Retired

1. Standards Published
   - October

2. Standards Effective
   - January 1

5. Old Standards Retired
   - December 31

6. Feedback Review
   - April–August

7. Draft Revisions
   - November–April

8. Final Review
   - May–July

YEAR 1

YEAR 2

YEAR 3

COMMUNITY MEETINGS
- September–October

Market Implementation
- All Year

Feedback Begins
- November
Stage 6 – Feedback Review

1. Standards Published
   October

2. Standards Effective
   January 1

3. Market Implementation
   All Year

4. Feedback Begins
   November

5. Old Standards Retired
   December 31

6. Feedback Review
   April–August

7. Draft Revisions
   November–April

8. Final Review
   May–July

YEAR 3
COMMUNITY MEETINGS
September–October

YEAR 1
COMMUNITY MEETINGS
September–October

YEAR 2
COMMUNITY MEETINGS
September–October

PCI Security Standards Council
Evolving Technology
Guidance and Threats
Provide and Evaluate
DSS & PA-DSS
Stage 7 – Draft Revisions

1. Standards Published
   October

2. Standards Effective
   January 1

3. Market Implementation
   All Year

4. Feedback Begins
   November

5. Old Standards Retired
   December 31

6. Feedback Review
   April–August

7. Draft Revisions
   November–April

8. Final Review
   May–July

COMMUNITY MEETINGS
September–October

Evaluating
Technology

Evolving
Technology

PCI
Security
Standards Council
Ongoing Evaluation

YEAR 1
- Standards Published
  - October
- Standards Effective
  - January 1
- Market Implementation
  - All Year

YEAR 2
- Old Standards Retired
  - November
- Feedback Begins
  - November
- COMMUNITY MEETINGS
  - September–October

YEAR 3
- Final Review
  - May–July
- Draft Revisions
  - November–April
- COMMUNITY MEETINGS
  - September–October

Guidance and Threats
Evaluate
Provide
Evolving Technology
PCI Security Standards Council
DSS & PA-DSS
Lifecycle for Changes to PTS

1. Standard Published
   - October

2. Feedback and Review
   - All Year

3. Standard Effective
   - January 1

4. Feedback and Review
   - All Year

5. Old Standard Retired
   - December 31

6. Draft Revisions
   - November–April

7. Market Review
   - May–June

8. Final Review
   - July–August

COMMUNITY MEETINGS
- September–October

Update #1 (If Required)
- June–August

Update #2 (If Required)
- June–August

YEAR 1
- Evolving Technology
- Provide Guidance
- Evaluate

YEAR 2
- Evolving Technology
- Provide Guidance
- Evaluate

YEAR 3
- Evolving Technology
- Provide Guidance
- Evaluate

PTS
- Lifecycle for Changes to PTS
Implementation
Need More Information?

www.pcisecuritystandards.org
Lifecycle for Changes to PCI DSS and PA-DSS

The Payment Card Industry Data Security Standard (PCI DSS) secures cardholder data that is stored, processed or transmitted by merchants and other organizations. The standard is managed by the PCI Security Standards Council (PCI SSC). Input for proposed changes to the standard is also made by PCI SSC stakeholders – Participating Organizations, including merchants, banks, processors, hardware and software developers, Board of Advisers, point-of-sale vendors, and the assessment (QSA & ASV) community.

Changes to the PCI standards follow a defined 36-month lifecycle with eight stages, described below. The lifecycle ensures a gradual, phased introduction of new versions of the standard in order to prevent organizations from becoming noncompliant when changes are published. This lifecycle also applies to the Payment Application Data Security Standard (PA-DSS), which covers validation requirements for applications used to process payment cards. During the lifecycle, the Council will continuously evaluate evolving technology and threats, and if necessary, make mid-lifecycle changes to the standards or provide ongoing supplemental guidance about these issues.

**NEW STANDARDS PUBLISHED**
- Major new release of PCI DSS and PA-DSS
- Presented at Community Meetings in September & October
- Initiates 3-year lifecycle
- Prior versions effective for 14 months

**Stage 1: Standards Published**
Stage 1 occurs in October of Year 1 after the Council’s annual Community Meetings and initiates a new lifecycle for the PCI DSS and the PA-DSS. Stakeholders may immediately implement the new standards, but are not required to do so until after they become effective.

**Stage 2: Standards Effective**
The second stage occurs on January 1 of Year 1. On this date, the new standards become effective. Stakeholders should begin using the new standards as the basis for their payment security programs. For purposes of validation for compliance, the old standards are grandfathered for 14 months. Nevertheless, the Council urges stakeholders to complete their transition to the new standards as quickly as possible, particularly where any new control requirements are critical for protecting cardholder data.

**Stage 3: Market Implementation**
During the third stage, the market completes its implementation of the new standards. This entails assessing changes to the new standards and determining their applicability to a stakeholder’s cardholder data environment. Stage 3 occurs throughout Year 1, which provides for an orderly, phased implementation of any required changes.

---

Lifecycle for Changes to PTS

The Payment Card Industry PIN Transaction Security (PTS) requirements are used primarily by point-of-sale equipment manufacturers to secure cardholder data at the physical point of sale. The standard is managed by the PCI Security Standards Council (PCI SSC). Input for proposed changes to the standard are also made by PCI SSC stakeholders – Participating Organizations, including merchants, banks, processors, hardware and software developers, point-of-sale vendors, and approved security evaluation laboratories.

Changes to the standard follow a defined 36-month lifecycle with eight stages, described below. The lifecycle ensures a gradual, phased use of new versions of the standard without invalidating current implementations of PTS. It also prevents organizations from becoming noncompliant when changes are published and allows vendors to complete existing product development. Throughout the lifecycle, the Council will continuously evaluate evolving technology and threats, and provide ongoing guidance about these standards.

**NEW STANDARDS PUBLISHED**
- Major new release of PTS
- Presented at Community Meetings in October
- Initiates 3-year lifecycle
- Prior versions remain effective for 12 months after the new standard becomes effective

**Stage 1: Standard Published**
Stage 1 occurs in October of Year 1 with the publication of the new standard; this initiates a new lifecycle for PTS. The new standard contains updates for ensuring an optimal level of security to the terminal for protecting cardholder data.

**Stage 2: Feedback & Review**
Stage 2 is an ongoing process of feedback and review occurring throughout Year 1. Feedback is actively sought from all Participating Organizations, security evaluation laboratories, the PCI PTS Working Group, and the PCI Security Standards Council. The goal is assessing the effectiveness and applicability of the new standard. Feedback can enable guidance for interpreting the standard, and how evaluation laboratories should collectively use similar methodologies for testing identical solutions.

If a new threat represents a significant security risk, the PCI Security Standards Council will take immediate action to help stakeholders understand how to minimize the threat and protect cardholder data.
Council Resources

- Security standards and supporting documents
- Quick Reference Guide
- Searchable Frequently Asked Questions
- List of approved PED Labs, QSAs, ASVs, PA-QSAs,
- Education and outreach - e.g., fact sheets, webinars
- Participating membership, meetings, collaboration
- A global voice for the industry
• The three year lifecycle streamlines the standards development process by aligning DSS, PA-DSS and PTS on a similar three year schedule
  – Phased, orderly introduction of new versions of the standard prevents organizations from becoming noncompliant when changes are published
  – Longer time for stakeholders to implement standards
  – More time for members to submit feedback
  – Additional time to consider market dynamics, emerging threats and new technologies before issuing new version
  – Greater transparency into the development process, makes sure there are no surprises
Thank You