



Security
Standards Council

The PCI Security Standards Council

7/20/07

Agenda

- The PCI SSC
 - Roles and Responsibilities
- How To Get Involved
- PCI SSC Vendor Programs
- PCI SSC Standards
 - PCI DSS Version 1.1
 - Revised SAQ



Security
Standards Council

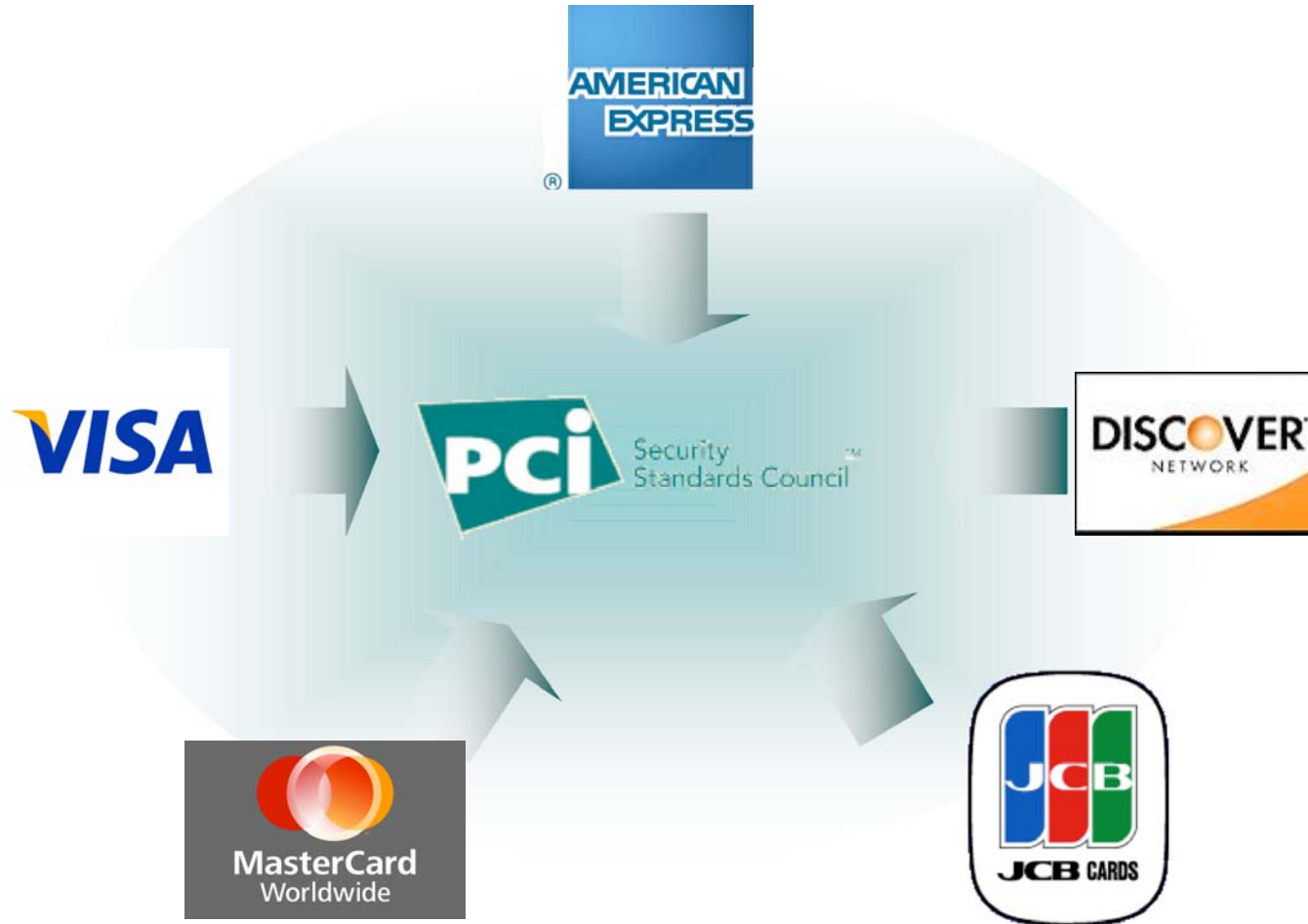
The PCI SSC

7/20/07

The PCI Security Standards Council

- An open global forum, launched in September 2006, for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

The PCI Security Standards Council Members



PCI Security Standards Council Objectives

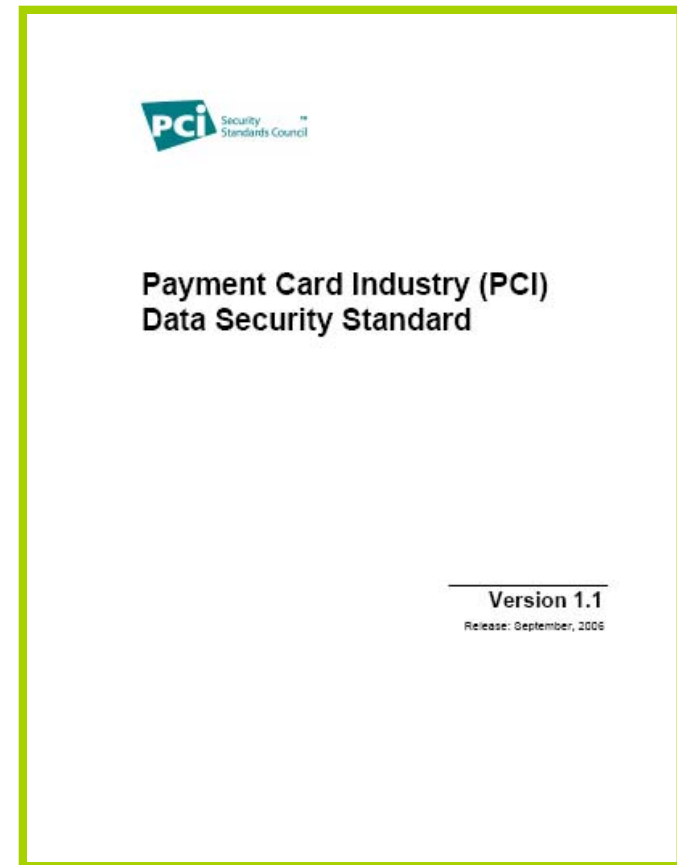
- Issue new standards
- Enhance payment account security
- Create awareness and drive adoption
- Foster participation and gather feedback
- Manage the qualification and approval testing process for ASVs and QSAs
- Maintain a current list of approved QSAs and ASVs

The PCI Data Security Standard

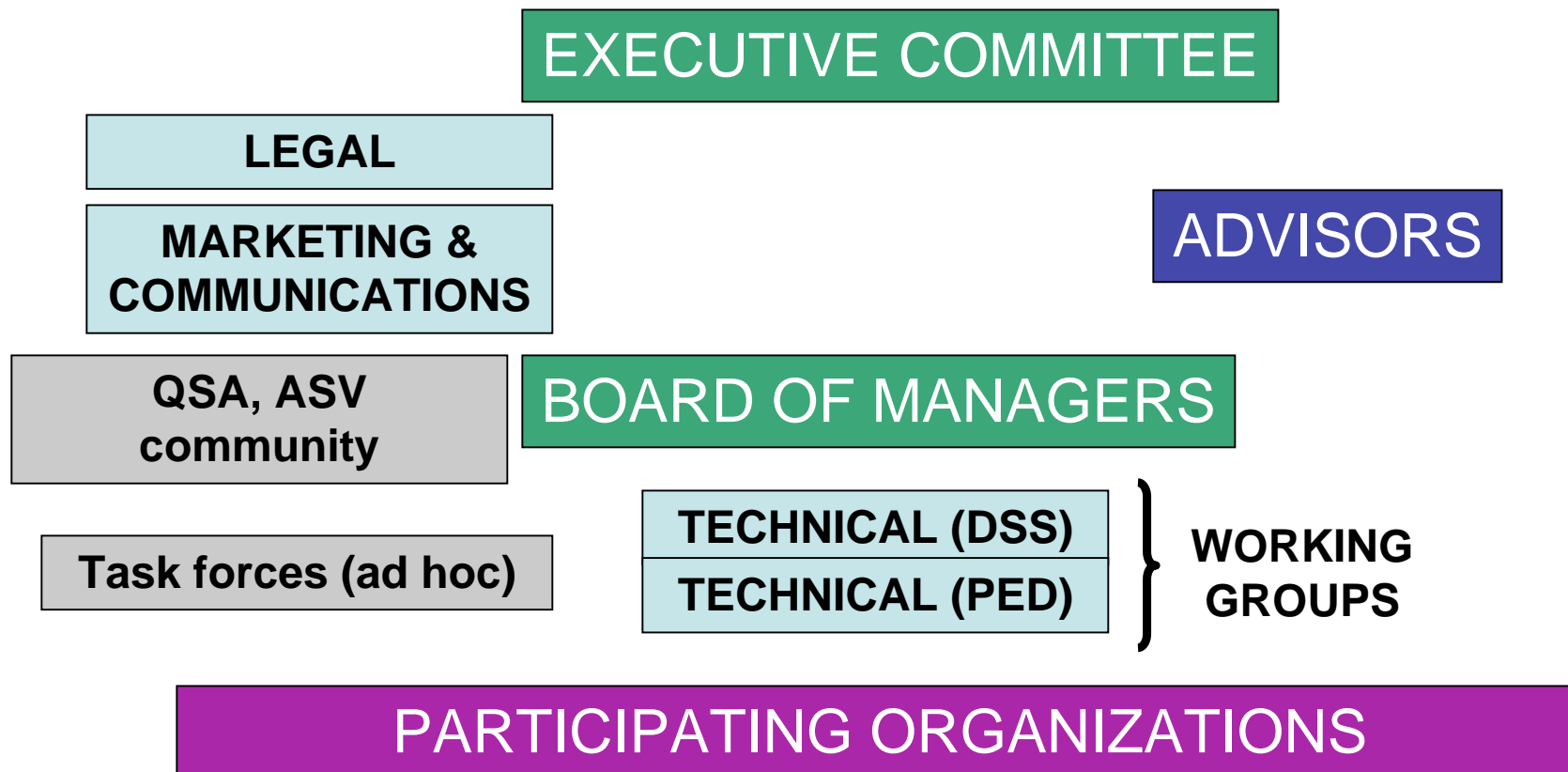
The PCI DSS version 1.1 is a set of comprehensive requirements for enhancing payment account data security.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

This comprehensive standard is intended to help organizations proactively protect customer payment data.



Organizational Structure





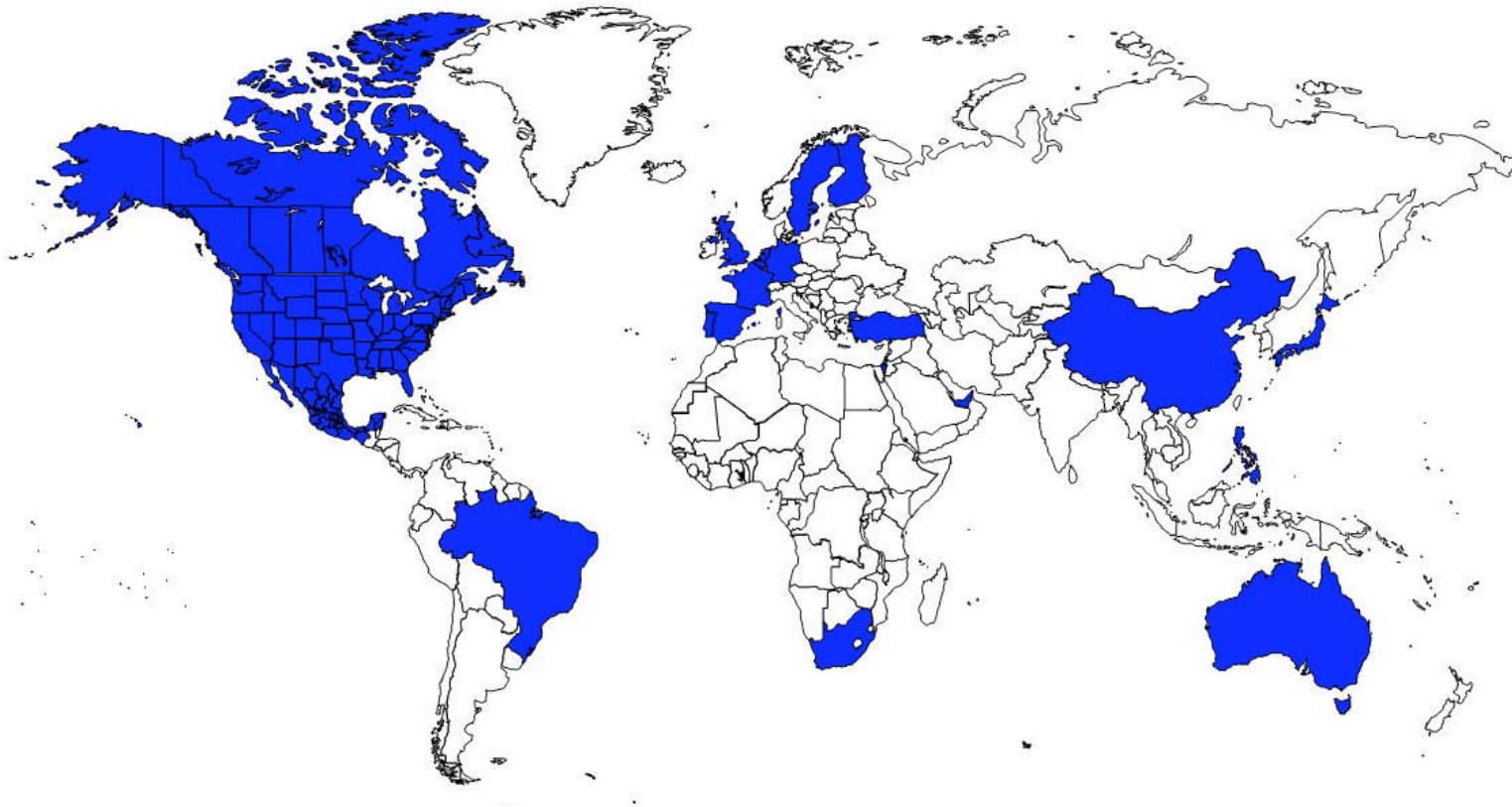
Security
Standards Council

How To Get Involved

7/20/07

Global Participation & Representation

Over 250 organizations have been accepted



A Seat at the Table, Board Representation & SIGs

- Financial Institutions
- Merchants
- Gateways
- Processors
- Service Providers
- EFT Networks
- Associations
- Vendors

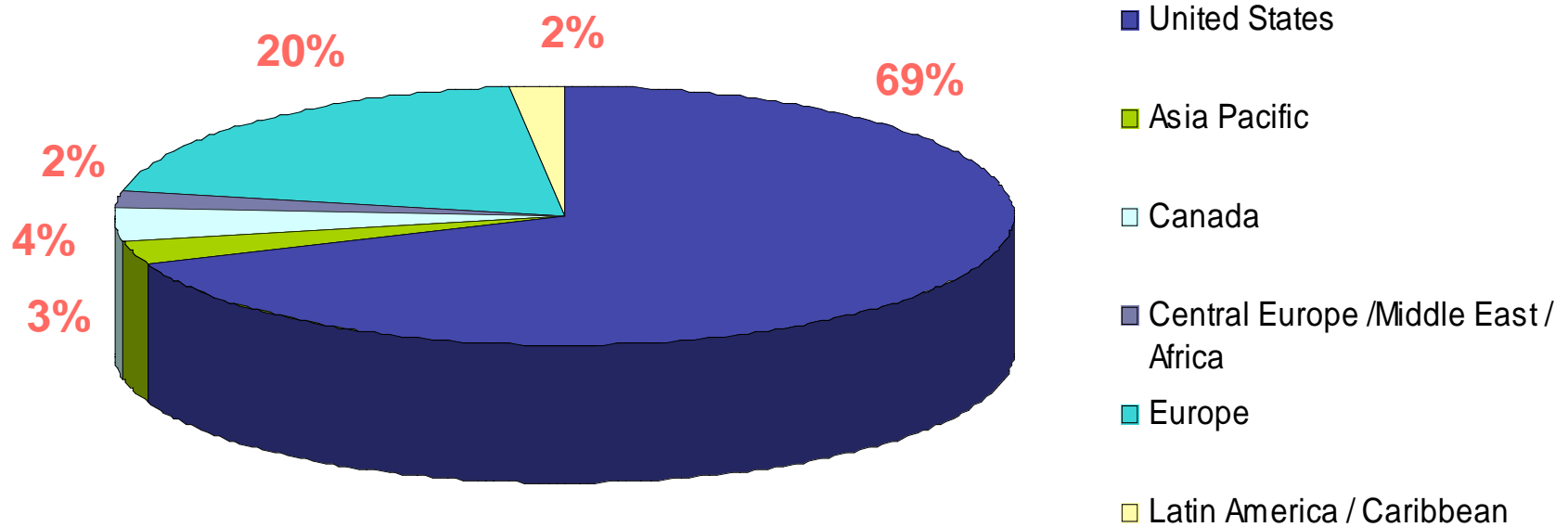


Participating Organization Privileges

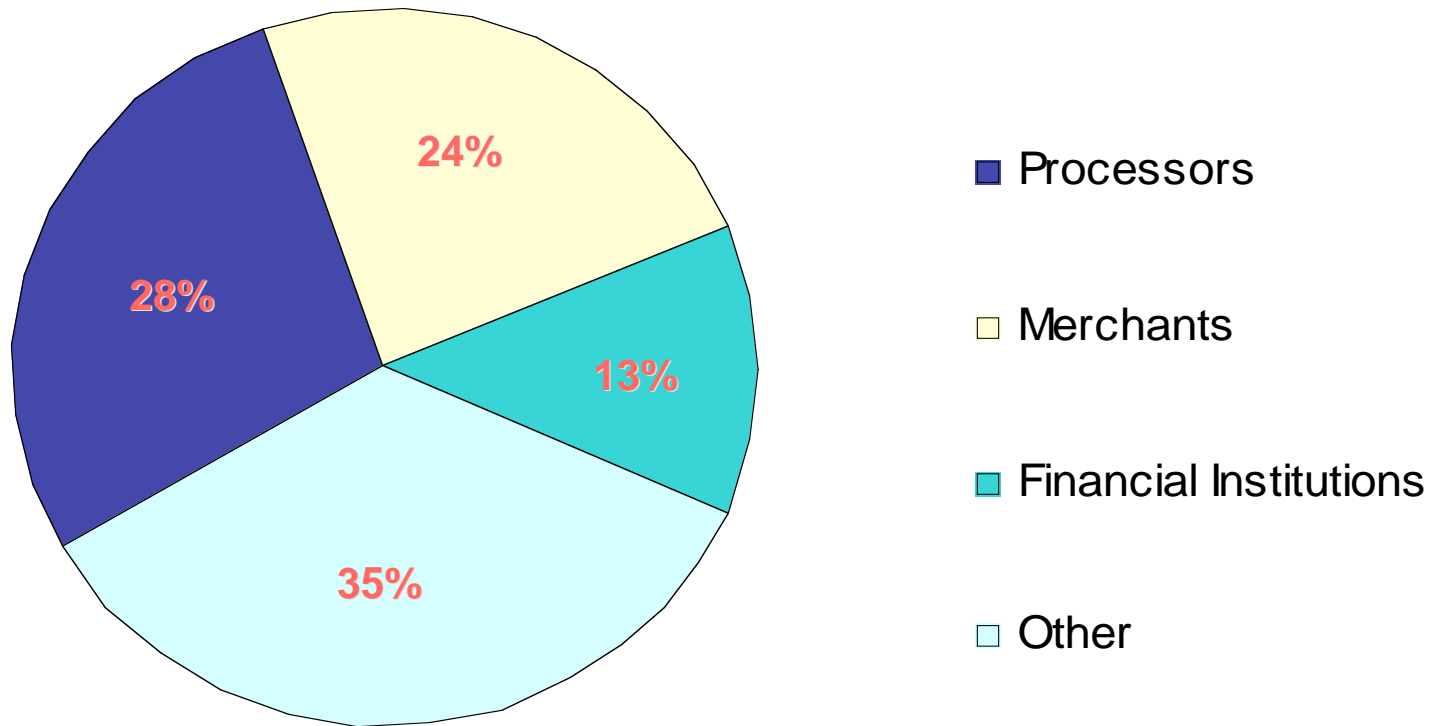
- Vote and Run for Participating Organization Board of Advisors.
- Comment on DSS, SAQ, PED and on other PCI SSC documentation, prior to public release.
- Attend Annual Community Meetings
- Attend Quarterly Webinar Meetings
- Recommend new initiatives and standards

Reserve Your Seat at the Table

Participating Organizations Regions



Participating Organizations Categories



Board of Advisors

- Financial Institutions
 - Bank of America
 - JP Morgan Chase and Co
 - Citibank N.A., Global Consumer Group
 - Commonwealth Bank of Australia
 - The Royal Bank of Scotland

Board of Advisors

- Merchants
 - British Airways PLC
 - Exxon Mobil Corporation
 - McDonalds Corporation
 - Microsoft
 - Tesco Stores Ltd
 - Wal-Mart Stores, Inc

Board of Advisors

- Others
 - APACS
 - EPC
 - PayPal Inc
 - VeriFone, Inc

Board of Advisors

- Processors
 - Chase Paymentech Solutions
 - First Data Corporation
 - Interac Association
 - Moneris Solutions Corporation
 - **SERVICIOS ELECTRONICOS GLOBALES S.A. DE C.V.**
 - TSYS Acquiring Solutions

Roles & Responsibilities

- Provide Feedback
 - Set Strategy
 - Emerging Security Issues
 - Additional Standards
 - Evolving the Current Standard(s)
 - Set Agenda/Programs for Community Meetings
- Time Commitments
 - Face to Face Meetings (as needed)
 - Conference Calls (regularly scheduled)
- SME, Panelists, Moderator (Community Meetings/Webinars)
- Regional & Business Category Market Feedback
- Ad Hoc Working Groups

Board of Advisors (Working Groups)

PA –DSS Task Force

- Develop Best Practices into to Industry Standards
- Evolution of testing criteria in the applications
- Driving Marketplace adoption
- Members Include:
 - Paypal
 - Verifone
 - Moneris
 - JP Morgan Chase

Community Meeting Agenda Task Force

- Restructure Agenda
- Define clear business models to use going forward
- Members Include:
 - Paypal
 - TSYS Acquiring Solutions
 - Microsoft
 - RBS

Outreach and Education Task Force

- Identify additional marketing and educational needs, based on industry size, region, etc.
- Members Include:
 - Walmart Stores Inc.
 - APACS
 - British Airways
 - First Data Corporation

Community Meeting





Security
Standards Council

PCI SSC Vendor Programs

7/20/07

QSAs

- Organizations that validate an entity's adherence to PCI DSS requirements are known as Qualified Security Assessors (QSAs).
- Nearly 90 QSA companies
- https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm

ASVs

- Organizations that validate adherence by performing vulnerability scans of internet facing environments of merchants and service providers are known as Approved Scanning Vendors (ASVs).
- Nearly 140 ASVs
- https://www.pcisecuritystandards.org/resources/approved_scanning_vendors.htm



Security
Standards Council

PCI SSC Standards

7/20/07

How has the PCI DSS changed ?

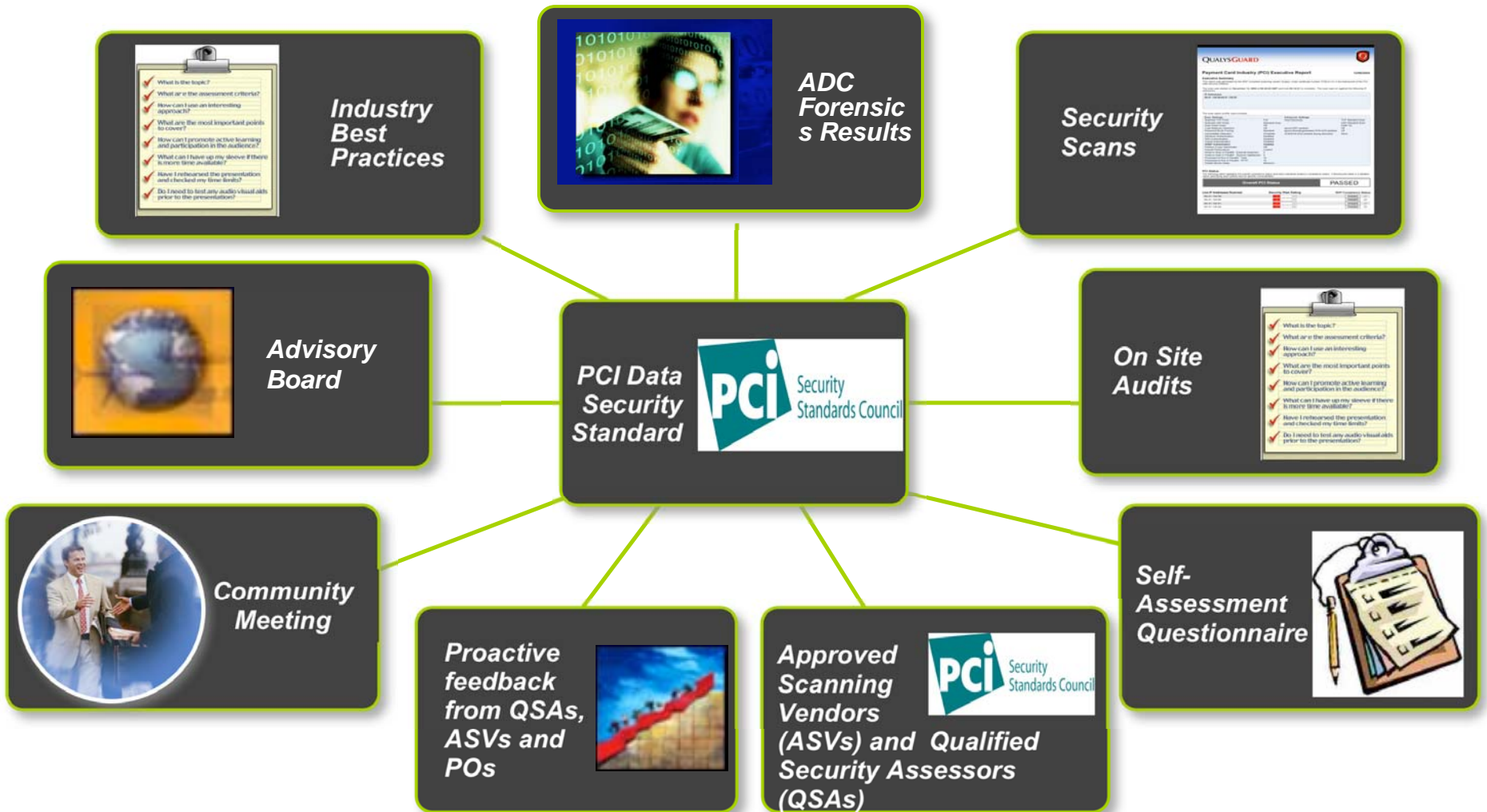
Updates are designed to foster broad adoption by acknowledging practical implementation issues, incorporating partner and customer feedback, while maintaining the robustness of security measures

- PCI DSS v1.1 revisions provide:
 - Clarification and consistency
 - Flexibility for technology or business constraints
 - Additional measures to address latest attack trends

PCI DSS v1.1 – Revision examples

- **Clarity and Consistency:**
 - Incorporated a clarification of data definitions, distinguishing between cardholder data that must be protected by PCI vs. sensitive authentication data that must never be stored
- **Flexibility:**
 - Defined compensating controls for data encryption, and provided ability for compensating controls to be applied to various requirements based on technical and business constraints
- **New Security Requirement:**
 - Created new application level requirement (6.6) to address significant trend in account data compromise cases, effective date June 30, 2008

PCI DSS Drivers



Frequently Asked Questions



- Over 800 questions submitted to TWG by QSAs, ASVs and Merchants
- Responses developed by all five payment brands help “pave-the-way” for PCI DSS evolution
- *Technical FAQ available on PCI SSC website in 3Q 2007*

New SAQ Objectives

- Alignment with the PCI DSS v1.1
- Based on industry feedback
- Flexibility for multiple merchant types
- Providing guidance for the intent and applicability of the underlying requirements
- May be used as a basis for an automated tool in the future

PCI DSS v1.1 - Revisions

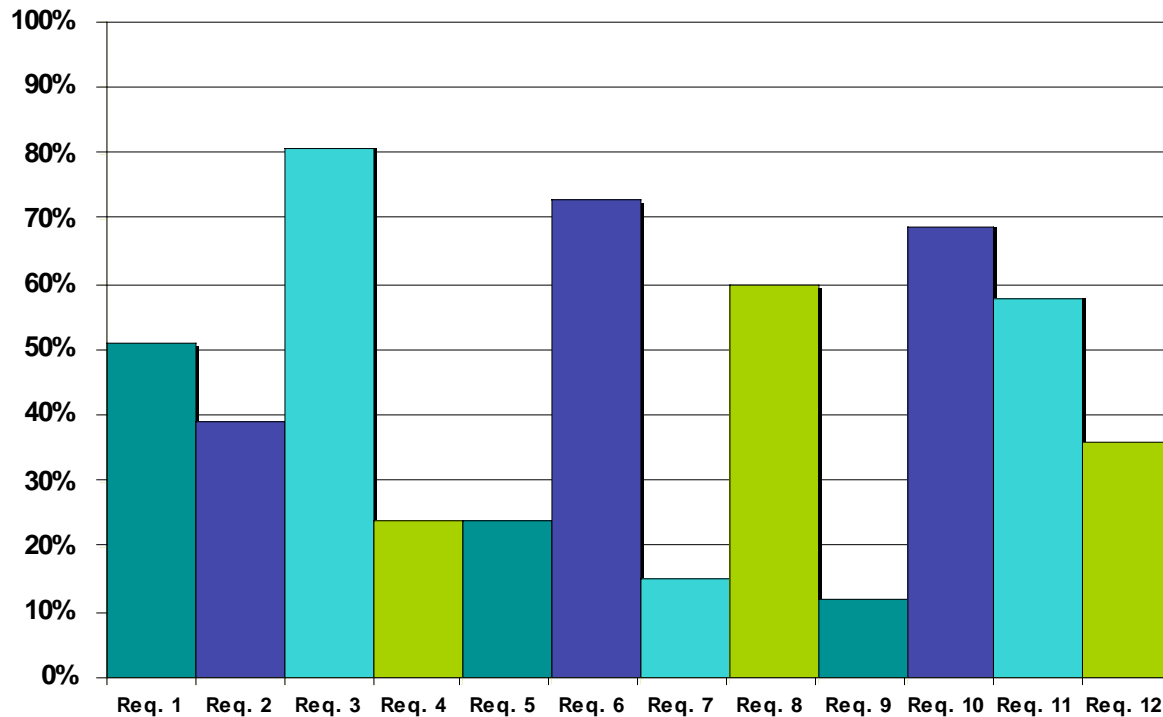
- Created new application level requirement (6.6) to address latest trend in account data compromise, implementation date set for June 30, 2008
- Incorporated a clarification of data definitions, distinguishing between cardholder data that must be protected by PCI vs. sensitive authentication data that must never be stored
- Defined compensating controls for data encryption
- Provided flexibility for compensating controls to be applied to various requirements based on technical and business constraints

PCI Update - Data Storage Clarification

	Component	Storage Permitted	Protection Required	Encryption Required**
Cardholder Data	PAN	YES	YES	YES
	Expiration Date*	YES	YES	NO
	Service Code*	YES	YES	NO
	Cardholder Name*	YES	YES	NO
Sensitive Authentication Data	Full Magnetic Strip	NO	N/A	N/A
	CVC2/CVV/CID	NO	N/A	N/A
	PIN	NO	N/A	N/A

* Data elements must be protected when stored in conjunction with PAN

Most Common PCI Requirements Not Met



**Percentage of Compromised Merchants That Failed To Meet Each PCI DSS Requirement*

***Data gathered from more than 170 card compromise investigations conducted by ATW**

Requirement 1:

- Install and maintain a firewall to protect cardholder data

Requirement 3:

- Protect stored data

Requirement 6:

- Develop and maintain secure systems and applications

Requirement 8:

- Assign a unique ID to each person with computer access

Requirement 10:

- Track and monitor access to network and card data

Requirement 11:

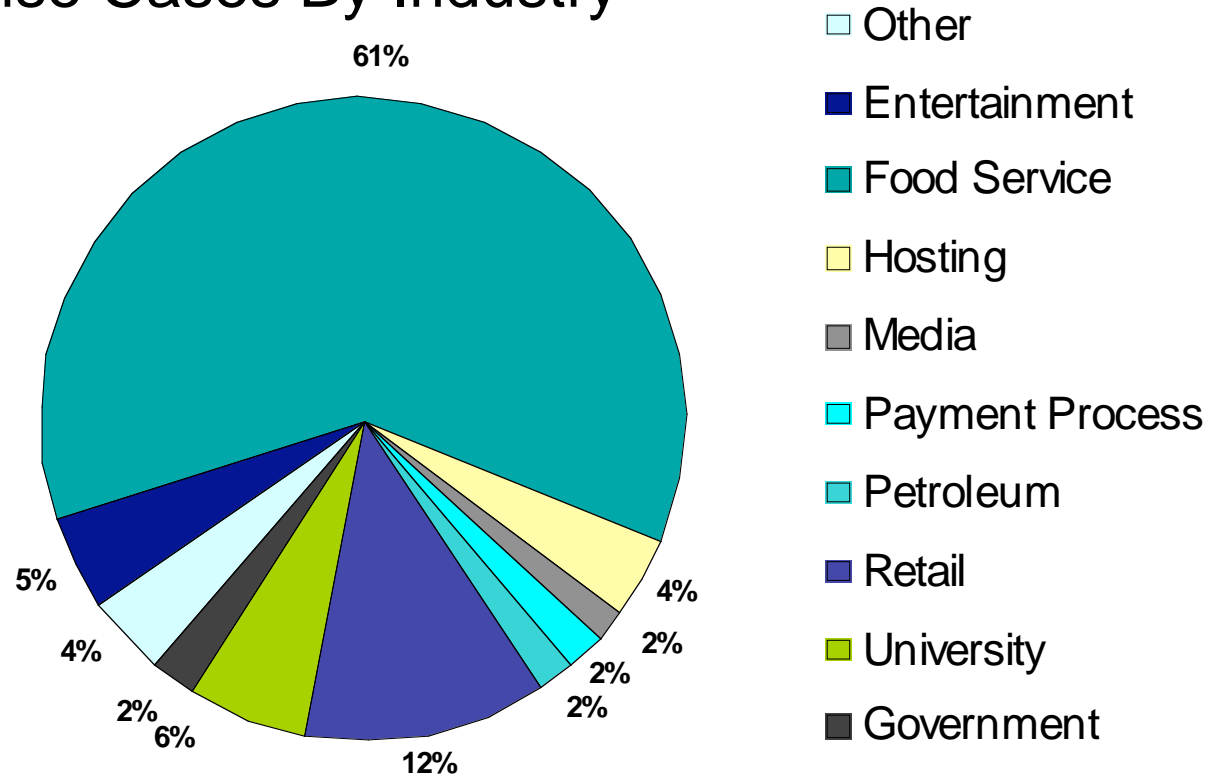
- Regularly test security systems and processes

Food Industry is Most Often Compromised

- Compromise Cases By Industry

“Other” includes:

- Recreational
- Professional organizations
- Transportation
- Travel
- Financial



*Data gathered from more than 170 card compromise investigations conducted by ATW

New Application Level Requirement

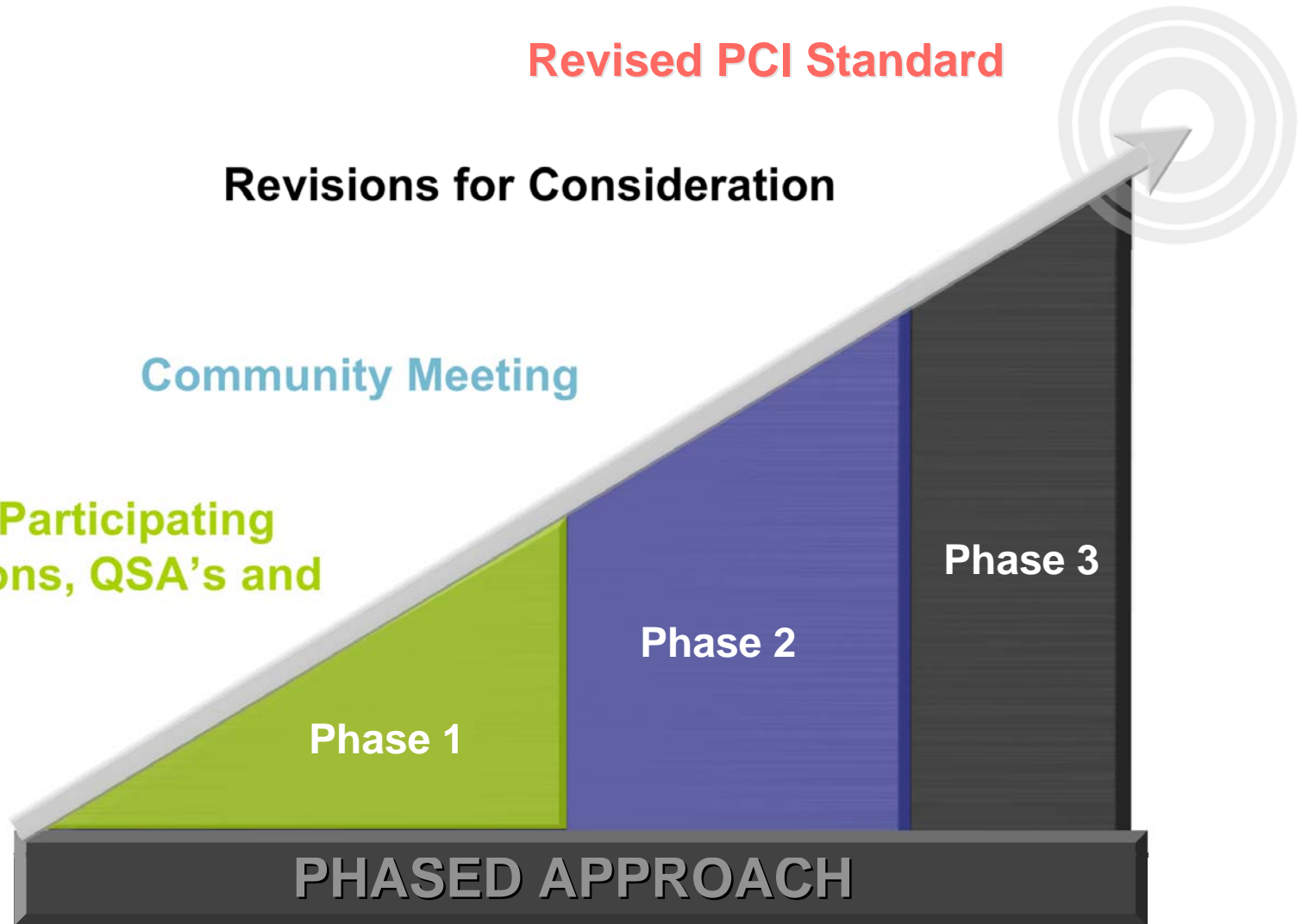
- Addresses SQL injection, cross-site scripting and other application level attacks
- Complements existing requirements for secure coding of web applications (6.5) and application level penetration testing (11.3.2)
- Seeks to provide added assurance that sites are not vulnerable, by either of the following methods:
 - Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security.
 - Installing an application layer firewall in front of web-facing applications

Revised PCI Standard

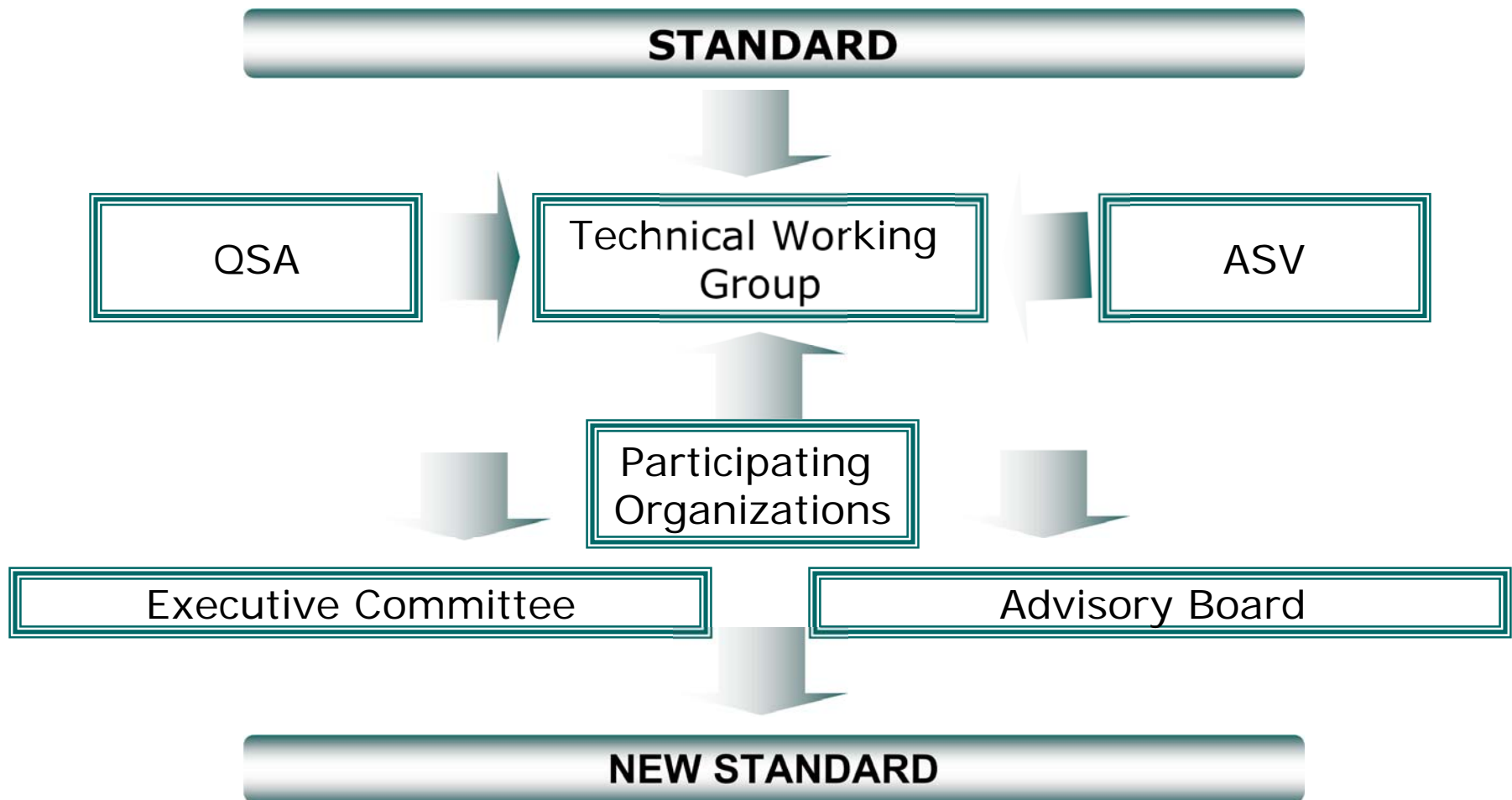
Revisions for Consideration

Community Meeting

Input from Participating Organizations, QSA's and ASV's



Revising the Data Security Standard



For more information

- Questions about the standards or supporting documents:
info@pcisecuritystandards.org
- *Questions that require interpretation from the Council's subject-matter experts may reflect the input of all five founding payment brands. We appreciate your patience as we work to craft your specific and individualized answer.*



Security
Standards Council

Thank You!

7/20/07