PCI Security Standards Council

# The State of PCI

**Troy Leach, Chief Technology Officer**
**PCI Security Standards Council**

10/12/2009

# The PCI Security Standards Council

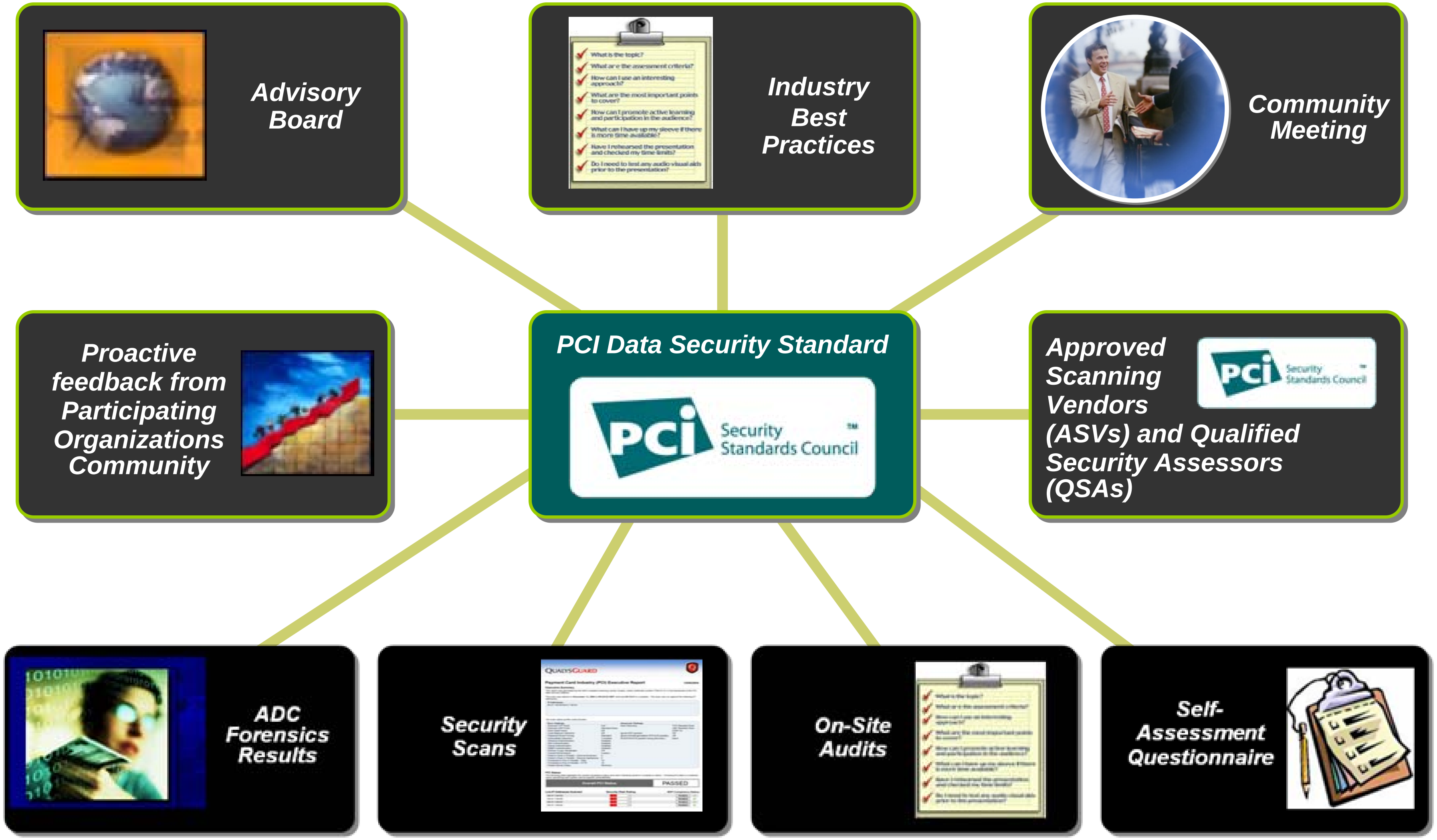
- An open global forum, launched in 2006, responsible for the development, management, education, and awareness of the PCI Security Standards, including:
  - Data Security Standard (DSS)
  - Payment Application Data Security Standard (PA-DSS)
  - Pin-Entry Device (PED)

PCI PED

PCI PA-DSS

PCI DSS

# PCI DSS Drivers


What is the topic?
What are the assessment criteria?
How can I use an interesting approach?
What are the most important points to cover?
How can I promote active learning and participation in the audience?
What can I have up my sleeve if there is more time available?
Have I rehearsed the presentation and checked my time limits?
Do I need to test any audio visual aids prior to the presentation?
PASSED

PCI Data Security Standard

Advisory Board

Industry Best Practices

Community Meeting

Proactive feedback from Participating Organizations Community

Approved Scanning Vendors (ASVs) and Qualified Security Assessors (QSAs)

ADC Forensics Results

Security Scans

On-Site Audits

Self-Assessment Questionnaire

# Roles and Responsibilities of the Council

## PCI SSC….

- Is an Independent Industry Standard
- Manages the technical and business  requirements for how payment data should be stored and protected
- Maintains List of Qualified PCI Assessors
  - QSAs, ASVs

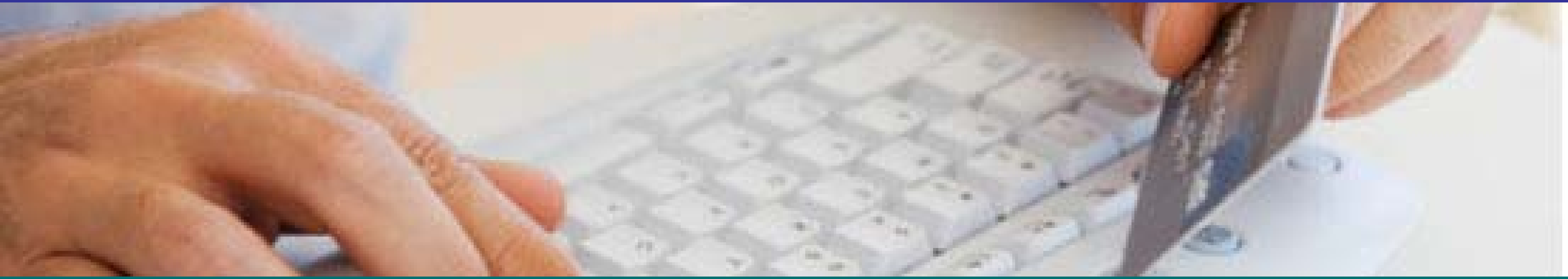
## PCI SSC Does Not…

- Manage or drive Compliance
  - Each brand continues to maintain its own compliance programs
    - Identifies stakeholders  that need to validate compliance
    - Definitions of Validation Levels
    - Fines and Fees

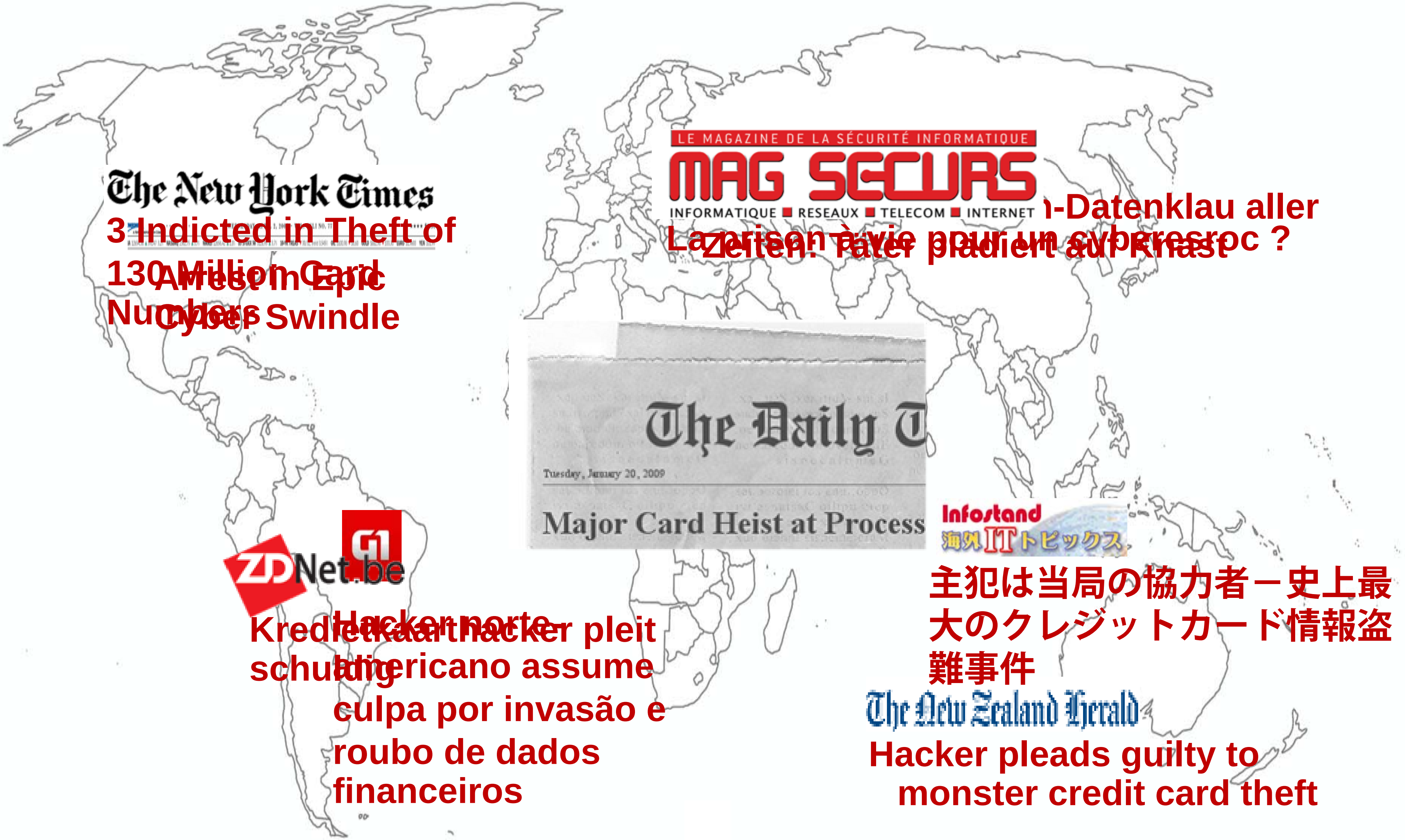
# 2009 PCI SSC Objectives

- Manage new and existing standards
- Operational Stability and Efficiency
- Enhance Stakeholder Engagement
- Training
- Expand Global Reach of PCI SSC

**Enhance cardholder data security**



# Global Headlines



The New York Times

3 Indicted in Theft of 130 Million Card Numbers

Arrest in Epic Cyber Swindle

LE MAGAZINE DE LA SÉCURITÉ INFORMATIQUE
MAG SECURS
INFORMATIQUE ■ RESEAUX ■ TELECOM ■ INTERNET

n-Datenklau aller Zeiten: Täter plädiert auf Knast

La prison à vie pour un cyberesroc ?

The Daily T

Tuesday, January 20, 2009

Major Card Heist at Process

ZDNet.be

Kredietkaarthacker pleit schuldig

G1

Hacker norte-americano assume culpa por invasão e roubo de dados financeiros

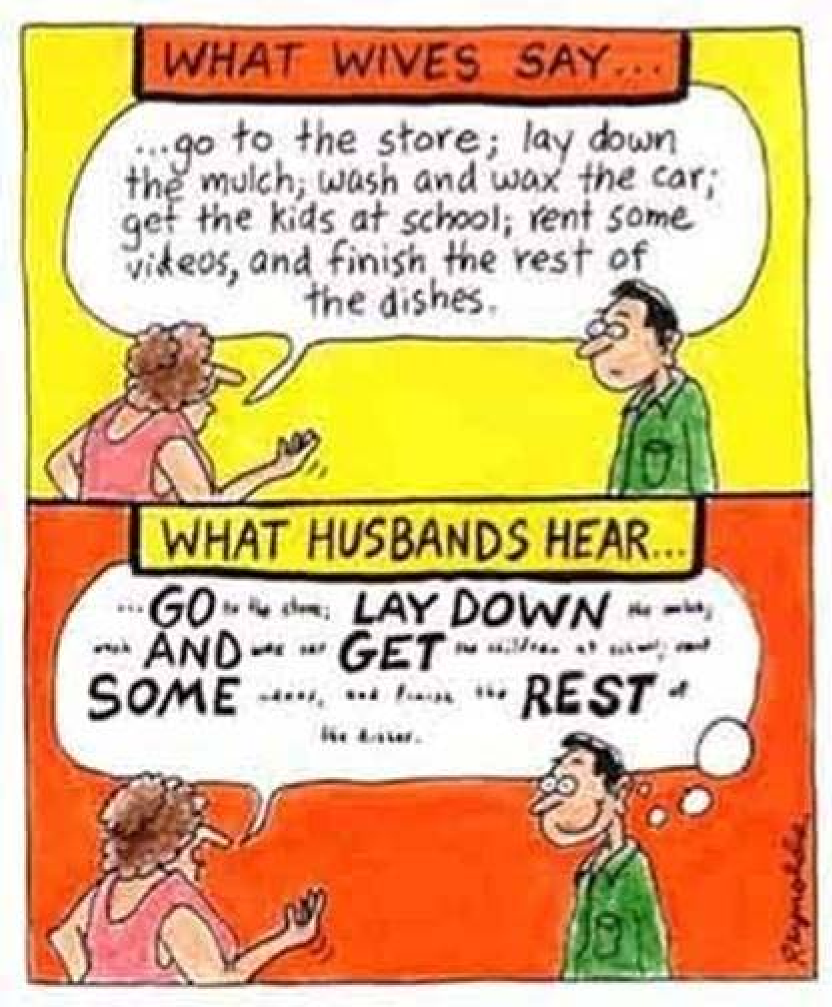
Infostand
海外ITトピックス

主犯は当局の協力者－史上最大のクレジットカード情報盗難事件

The New Zealand Herald

Hacker pleads guilty to monster credit card theft

# Communication


WHAT WIVES SAY...
...go to the store; lay down the mulch; wash and wax the car; get the kids at school; rent some videos, and finish the rest of the dishes.
WHAT HUSBANDS HEAR...
...GO to the store; LAY DOWN the mulch; wash AND wax the car GET the children at school; rent SOME videos, and finish the REST of the dishes.

# Did You Know?

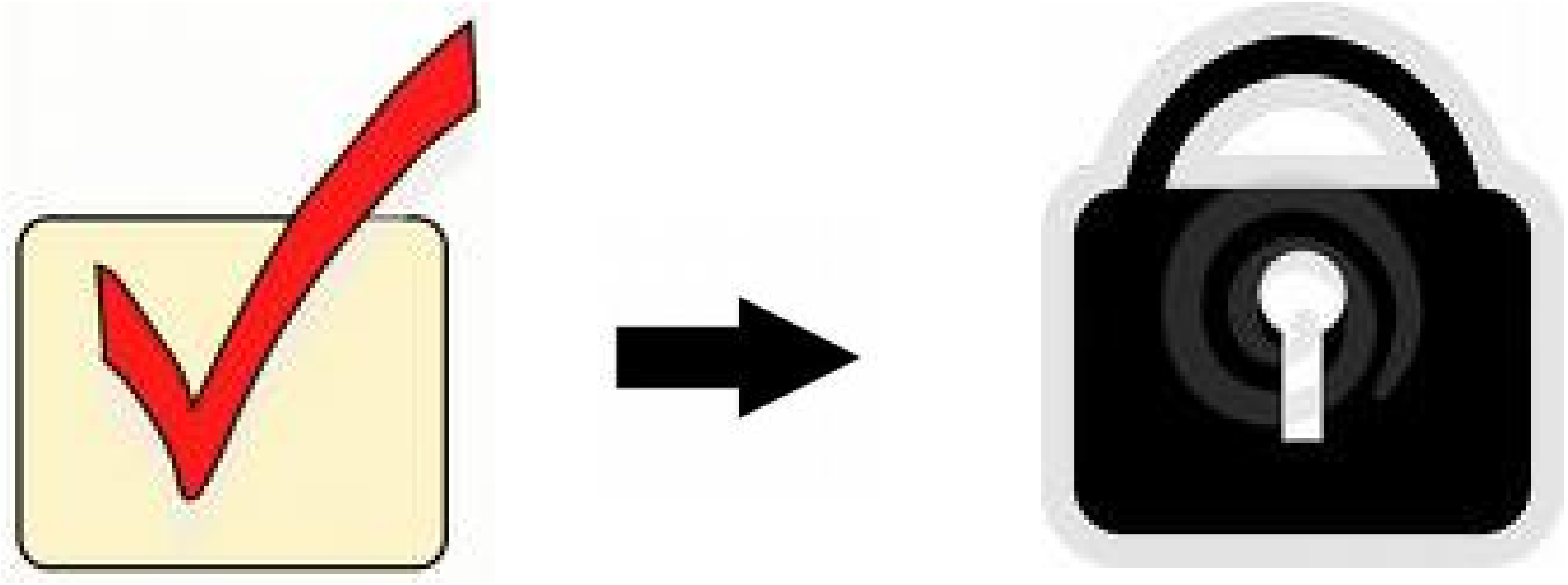
verizonbusiness

2009 Data Breach
Investigations Report

*According to Verizon's 2009 Data Breach Investigations Report (DBIR)*

- 75% of compromises were discovered at least weeks after the compromise.
- Post-breach reviews resulted in the discovery that:
  - – Breached organizations only had 11% compliance level for Req 3 (Protect card holder data).
  - – only 5% compliance level for Req 10 (track & monitor all access to network resources and cardholder data)

# Changing a mindset



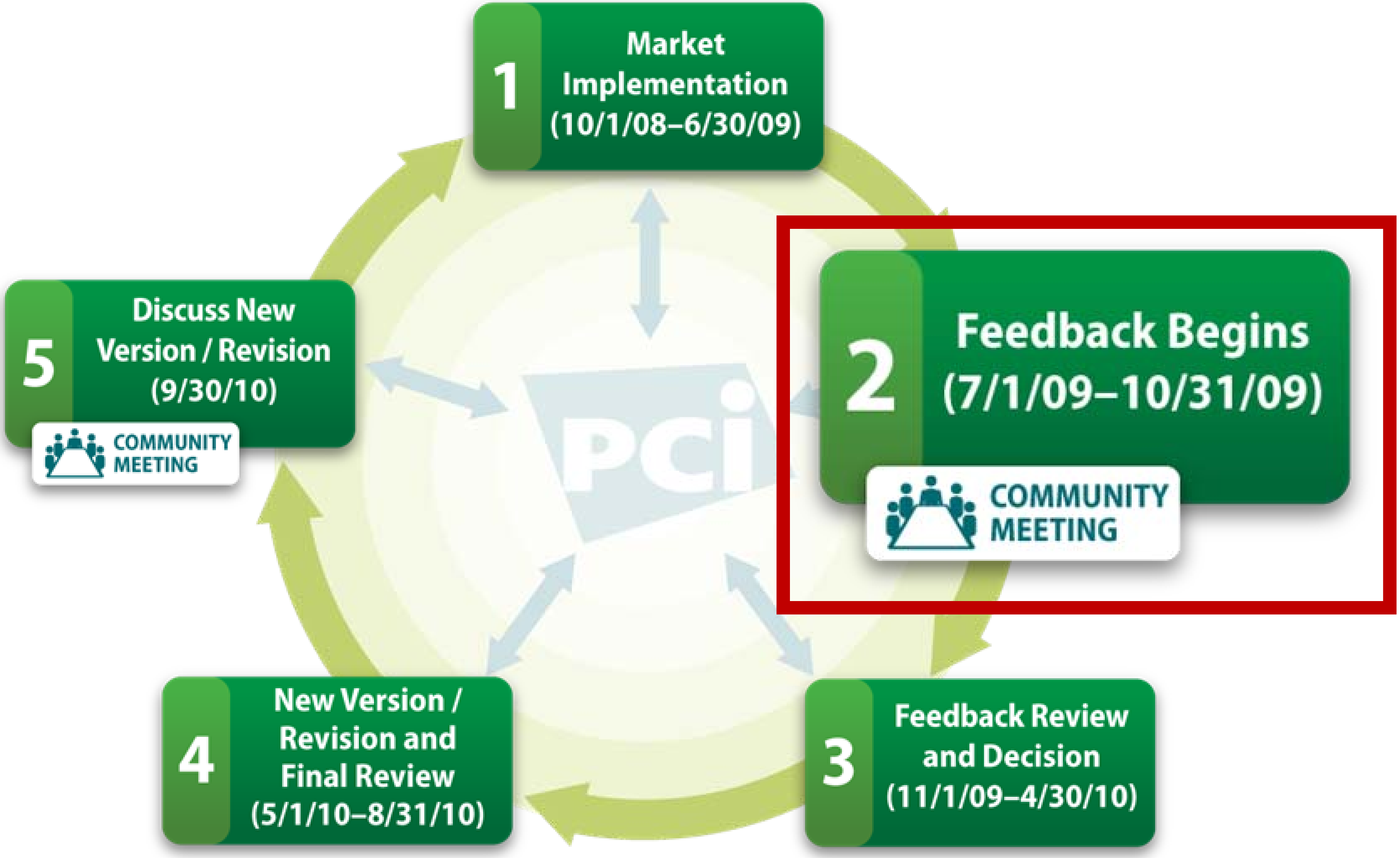
# Common Myths of PCI DSS

- One product will make us compliant
- Outsourcing processing makes us compliant
- PCI DSS compliance is an IT project
- PCI DSS will make us secure
- PCI DSS is unreasonable; it requires too much

# Common Myths of PCI DSS

- PCI DSS requires us to hire a QSA
- PCI DSS is only for high-volume transactions
- We completed a SAQ so we’re compliant
- We are required to store cardholder data
- PCI DSS is too hard

# What’s Next?



1 Market Implementation (10/1/08–6/30/09)

2 Feedback Begins (7/1/09–10/31/09)
COMMUNITY MEETING

3 Feedback Review and Decision (11/1/09–4/30/10)

4 New Version / Revision and Final Review (5/1/10–8/31/10)

5 Discuss New Version / Revision (9/30/10)
COMMUNITY MEETING

# What’s Next?

- **Research of Emerging Technologies**
- **Special Interest Groups**
  - **Wireless**
  - **Virtualization**
  - **Pre-Authorization**
  - **Scoping**
- **New education programs**
- **Additional standards**
- **Quality Assurance program**
- **2010 release of PCI DSS, PA-DSS and PTS**