

PCI Security as a Lifecycle: How to Plan for PCI in 2012 and Beyond

Bob Russo
**PCI SECURITY STANDARDS
COUNCIL**

Session ID: GRC-204

Session Classification: Intermediate

RSACONFERENCE2012

About the Council

Open, global forum

Founded 2006

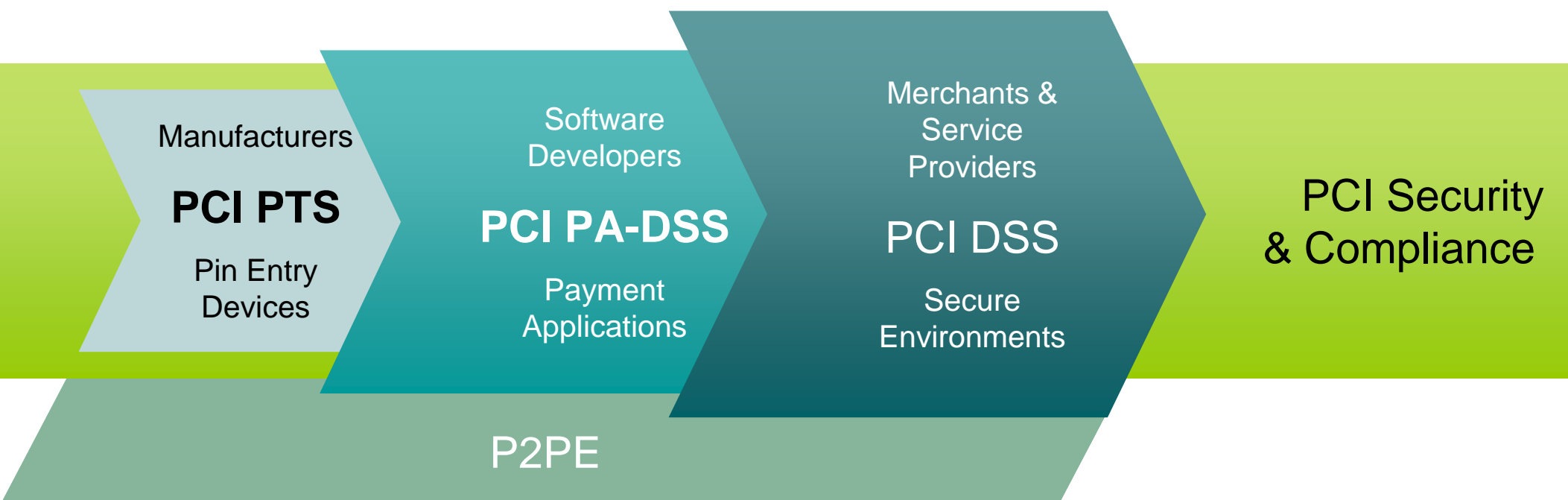
Responsible for PCI Security Standards

- Development
- Management
- Education
- Awareness



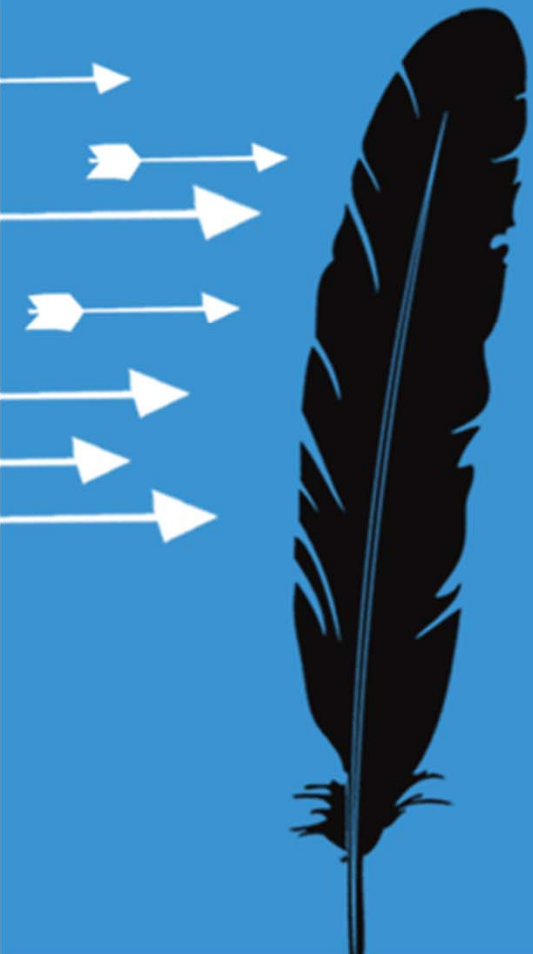
PCI Security Standards

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users





PCI Update

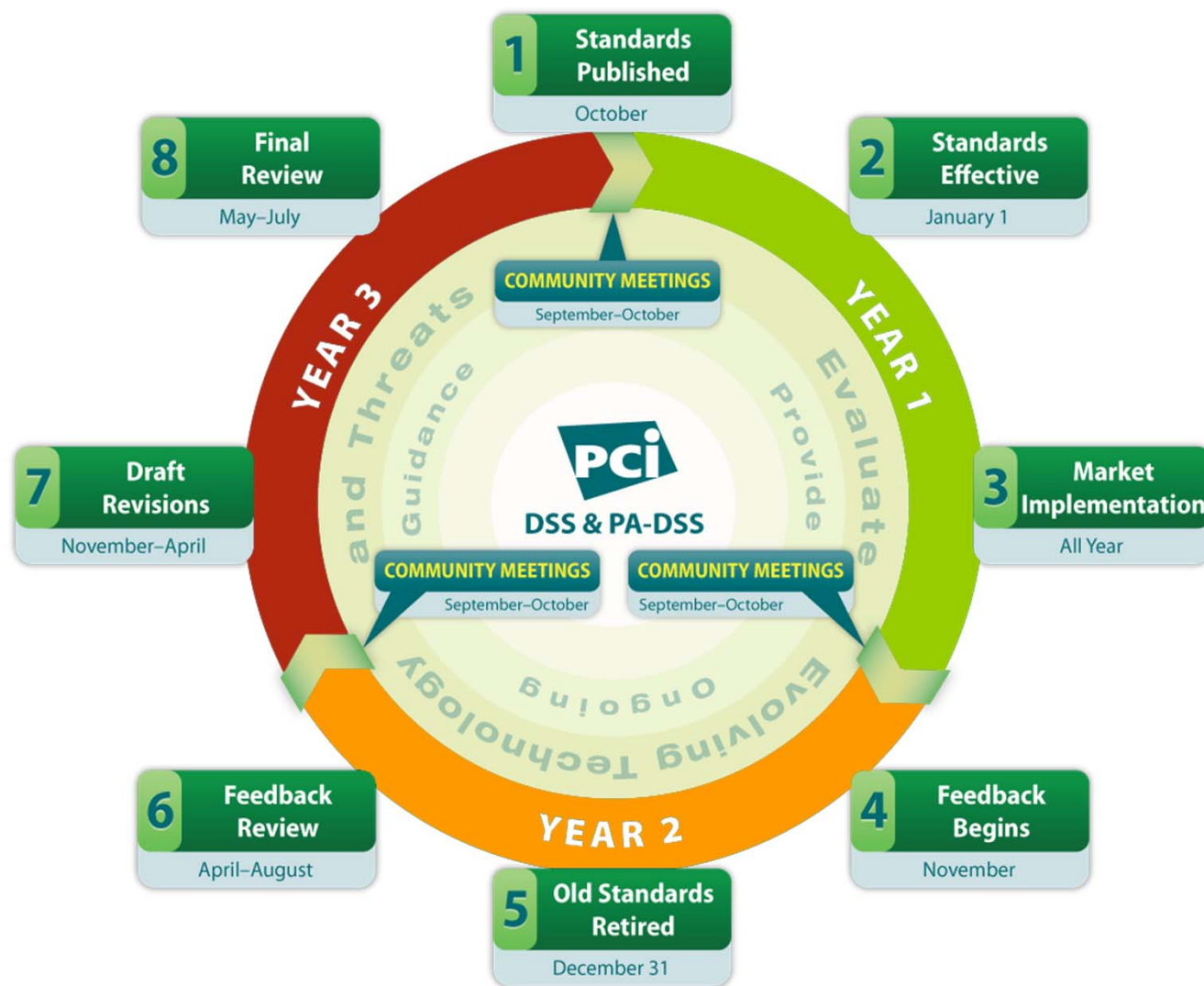
2012: Feedback Year

Submit feedback today
<https://programs.pcissc.org/>

Implementation
Feedback

Formal
Feedback

Draft Revisions
Feedback



POI Security Requirements V3.1



Errata

Standard 12-18 months after initial publication

P2P Support – Leverage Existing POI Criteria

Secure (Encrypting) Card Readers

Select Core and SRED Requirements

Non-PIN Entry Devices

Mandatory SRED module

Open Protocols (if applicable)



New Program - P2PE Hardware/Hardware



Point-to-Point Encryption (P2PE)

- The Council delivered *Initial Framework on Point-to-Point Encryption* guidance in October 2010
- P2PE solutions may help merchants reduce scope of their CDE and their PCI DSS assessment
- The Council now has the first set of P2PE validation requirements for hardware-based encryption and decryption solutions
- Developed with the Encryption Task Force
- Supporting testing procedures, assessor training, and other resources available in 2012



New Guidance - Mobile



PCI SSC Update June 2011 Mobile

Update & FAQ on applicability of PA-DSS to mobile payment acceptance applications

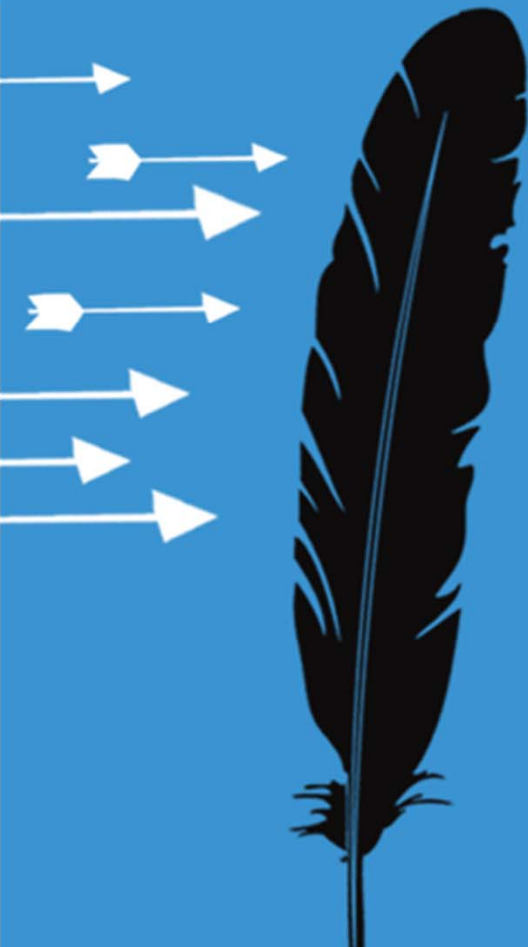
- Category 1 and 2 applications are eligible for PA-DSS
- Category 3 applications are pending development of further guidance and/or standards

Category 1
PTS Approved
PED Devices

Category 2
Purpose Built POS
Devices

Category 3
General Purpose
Smart Device





Planning ahead for
PCI by building a
security lifecycle
into your everyday
business

PCI Bridge of Compliance



Compliance



What is a PCI Lifecycle Approach



Reduce the
attack surface



Continuous
Awareness &
Protection



Prevent New
Types of
Exposure



Measure
success and
identify
opportunity



Lifecycle Principles Within PCI DSS & PA-DSS

The lifecycle process approach to information security management presented in ISO 27001 encourages users to:

- Understand your information security requirements
- Implement controls to manage overall business risks
- Monitor and review the performance and effectiveness of the controls
- Continual improvement based on objective measurement

Some examples from the PCI Standards

Req 6.3.7

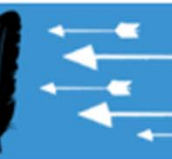
Req 11.2

Req 12.1

Why PCI DSS Requires Ongoing Risk Assessment

Technology innovation leads to new attack vectors

Consider the amount of business changes as well as technical



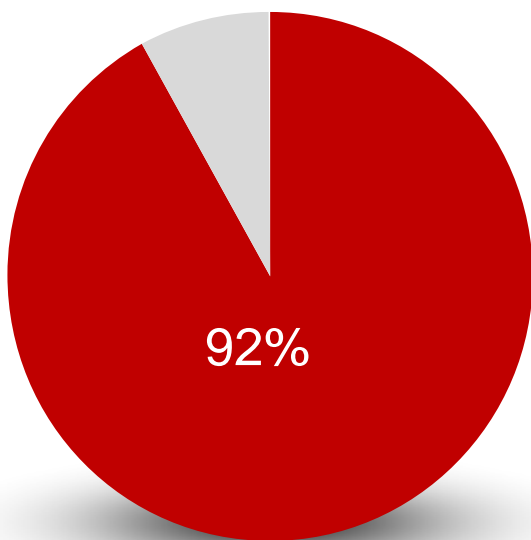
Easier Said Than Done

Why we fail to maintain secure environments

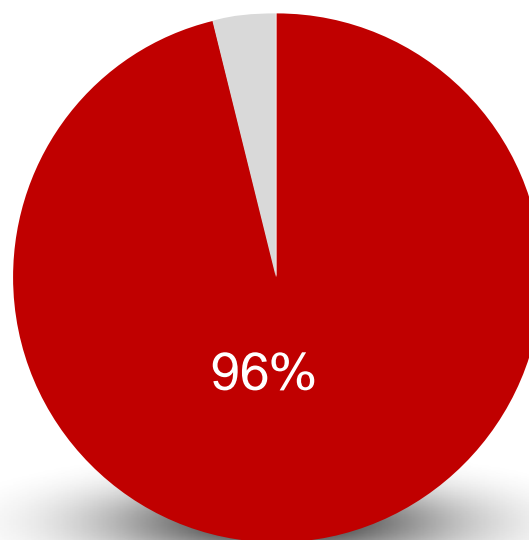
- Lack of awareness by IT practitioners
- Incentive to keep security a primary focus
- Quickly evolving technology landscape
- Rapid development and distribution of new solutions
- Still unnecessary exposure of CHD

Eliminate the Simple

92% of
compromises were
simple



96% were avoidable through
simple or intermediate
controls



Verizon Business 2011 Data Breach Investigations Report

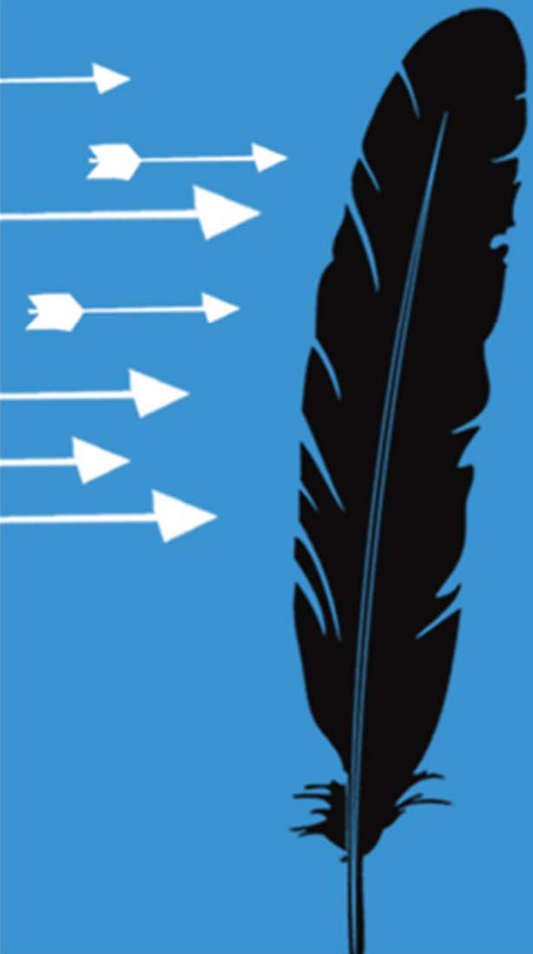


Results from a PCI Lifecycle

- PCI Lifecycle can prevent one mistake leading to mass data compromise
- PCI Lifecycle can minimize validation and improve security response



How to Implement a PCI Security Lifecycle



Reduce the Attack Surface



Continually identify the environment

Maintain a CHD
Dataflow Diagram

Meet regularly
with those able to
create cardholder
data pathways

DLP Methodology



Partner with Trusted Experts



Consider Payment Security Alliances

Trust but verify partners

Verify claims of PCI DSS compliance

Require agreements to maintain skillset

Verify all third-party access

Scope of Access:

- Approval Process
- Revocation Process
- Periodic Review



You Can't Attack What Isn't There



Confirm there is still need to retain

Verify with your financial
partners

Evaluate opportunities to use
surrogate values to replace
PAN



Management Commitment for Success



Don't let management think
the finish line was a compliant
ROC

Strategy for management
commitment

FINISH





IT Commitment for PCI Success

Strategy for having IT commit to PCI success

Engage IT in the threat modeling process

Security as Business Goal

Incentive to attend training annually

If your engineers do not know what constitutes a security bug, they will find none when reviewing their work



Building a PCI Leadership Team



Set objective metrics for success

Each PCI security coach should be able to translate threats into relevant questions for their group

Security should be a common skillset not confined only to PCI auditors

Assigning security advisors within your organization



Education and Awareness of your PCI Lifecycle



Strategy for on-going PCI training
and how to keep it fresh

Measuring retention of knowledge

Introduction to PCI
requirements

Trustworthy
computing

Basic security
design

Threat modeling &
Attack Surface
Analysis

Security Response



Practice Good Security Hygiene



Common Secure Development Principles

- Keep it simple
- Fail-safe default
- Open design
- Separation of privilege
- Minimize shared resources
- Localize Security



Prevent New Types of Exposure

Create a threat model for cardholder data

Use real-case scenarios

Identify dependencies (people, systems, services)

What security assumptions have you made?

Any updated information available externally?

Using that threat model as a gap analysis before your QSA or PA-QSA assessment



Defining and Following Best Practices

Have Clear Asset Identification of Payment Account Data

Are you asking the right questions?

How does the
cardholder data flow?

Where is there storage
of data?

Where is there
available connectivity?

Is all cardholder data
classified as such?

What are our
dependencies?

What features are
installed by default?



New things should come with warnings



Create Asset Identification for CHD

- Flag new systems and payment dataflows
- Flag when new privileged access is provided
- More closely monitor the behavior of new applications



Utilizing Policy



Creating and Executing Good Policy

Importance of the Implementation Guide

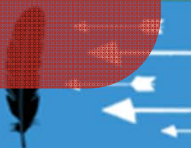
Creating tools to help

Enterprise
Application
Store

DLP
Methodology

Use Policy

ASV
Scanning



Testing the Policy



Test the
documentation

Re-evaluate the
policies

Have
environmental
values
changed?



Test the Strategy



Proactively look for updates

The Importance of Fuzzing

Default Passwords



Measure Success and Identify Opportunities



Examples of PCI Lifecycle metrics

Req 1

Number of systems with direct connectivity
Ratio of attacks per e-commerce sessions

Req 2

Number of accounts with no owners
Percentage of systems not patched within 30 days

Req 3

Percentage of systems containing cardholder data
Number of business units with access to cardholder data

Req 5

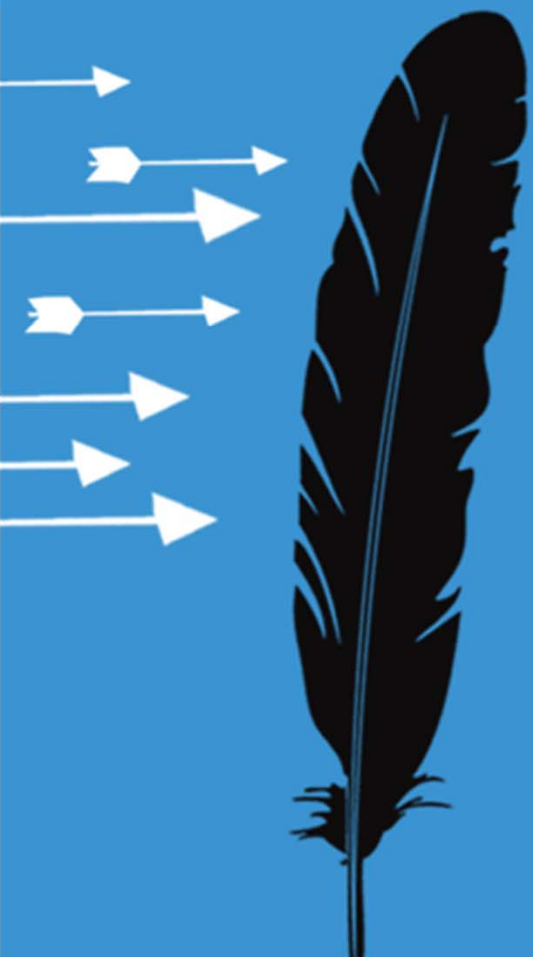
Percentage of systems with up-to-date signature files
Number of systems identified with malware

Req 11

Percentage of systems undergoing vulnerability scan
Percentage of external to internal servers with latent patches



How PCI Security Lifecycle can Simplify Compliance



May Discover Ways to Simplify the Process

Any exposure of cardholder data beyond acceptance?

Reduce number of departments and individuals with direct access



Simplify the Environment

*Remove
unnecessary
systems*

*Use compliant
service providers
and partners*



Simplify Payment Application Development

*Development team
aware of need to
protect data*

*Lab Validated
Applications*



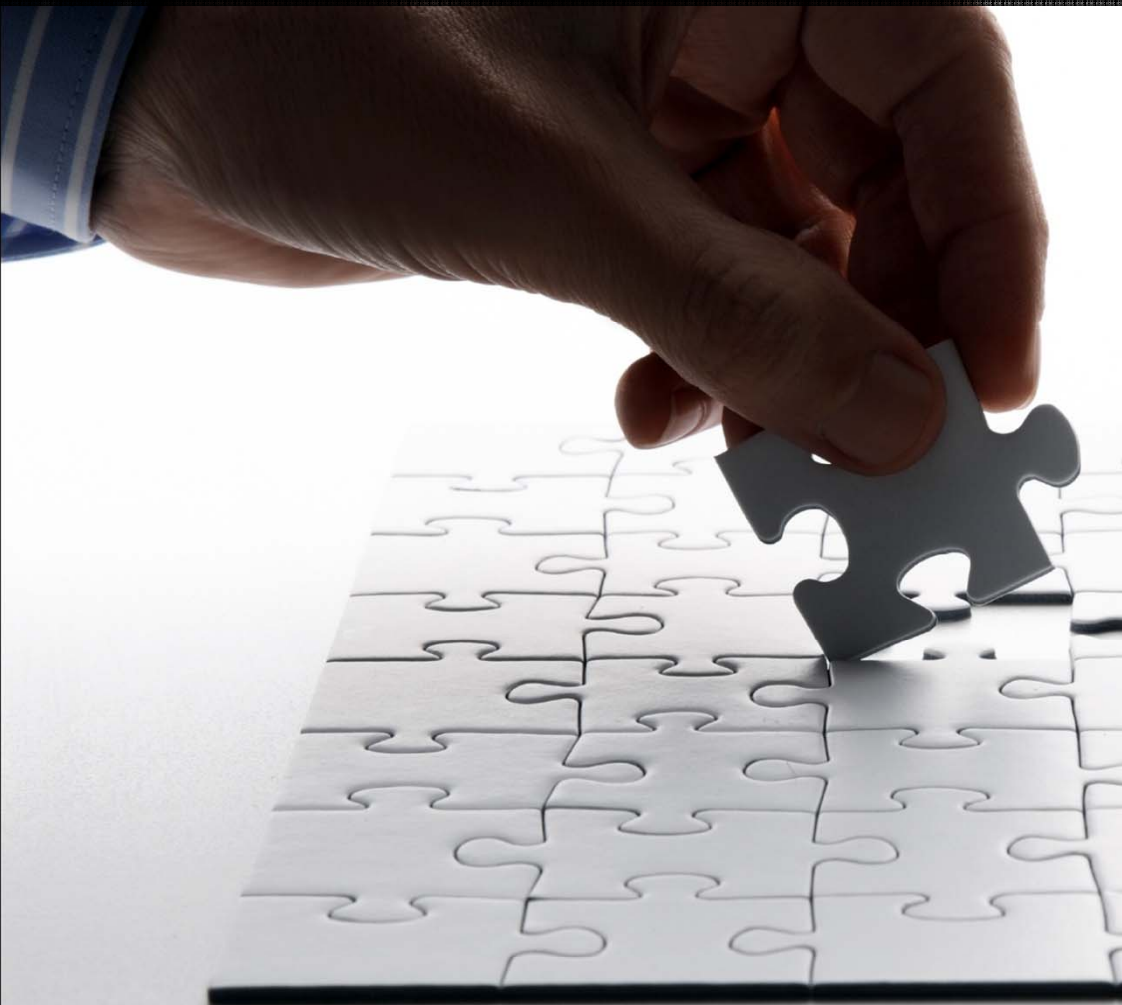
Simplify the Implementation

*Installation
consistently aligns
with policy*

*Installed to
specification by a
qualified professional*



Use of Trusted Devices



*Lab Accredited
Devices*

*Aware of skimming
attacks*

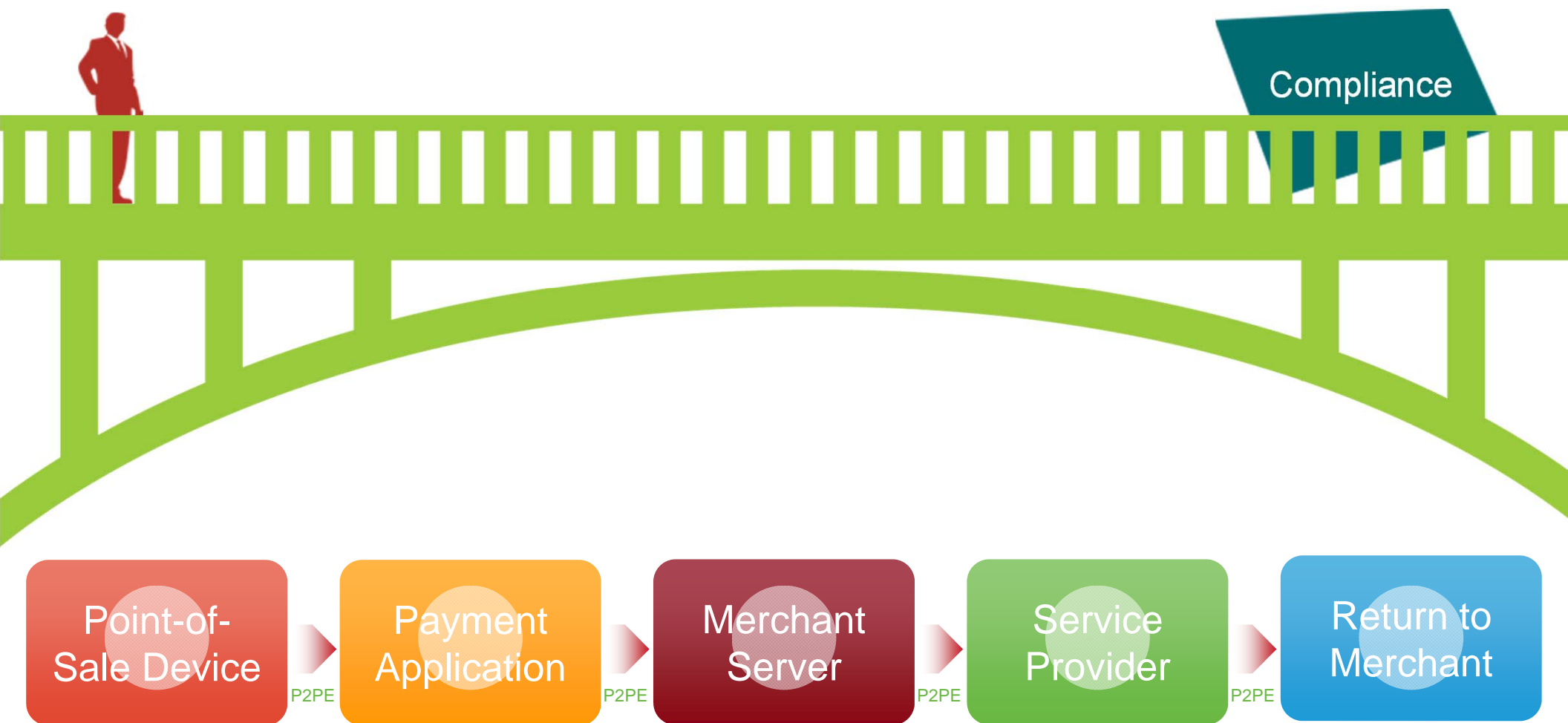


What the Council is Doing to Help

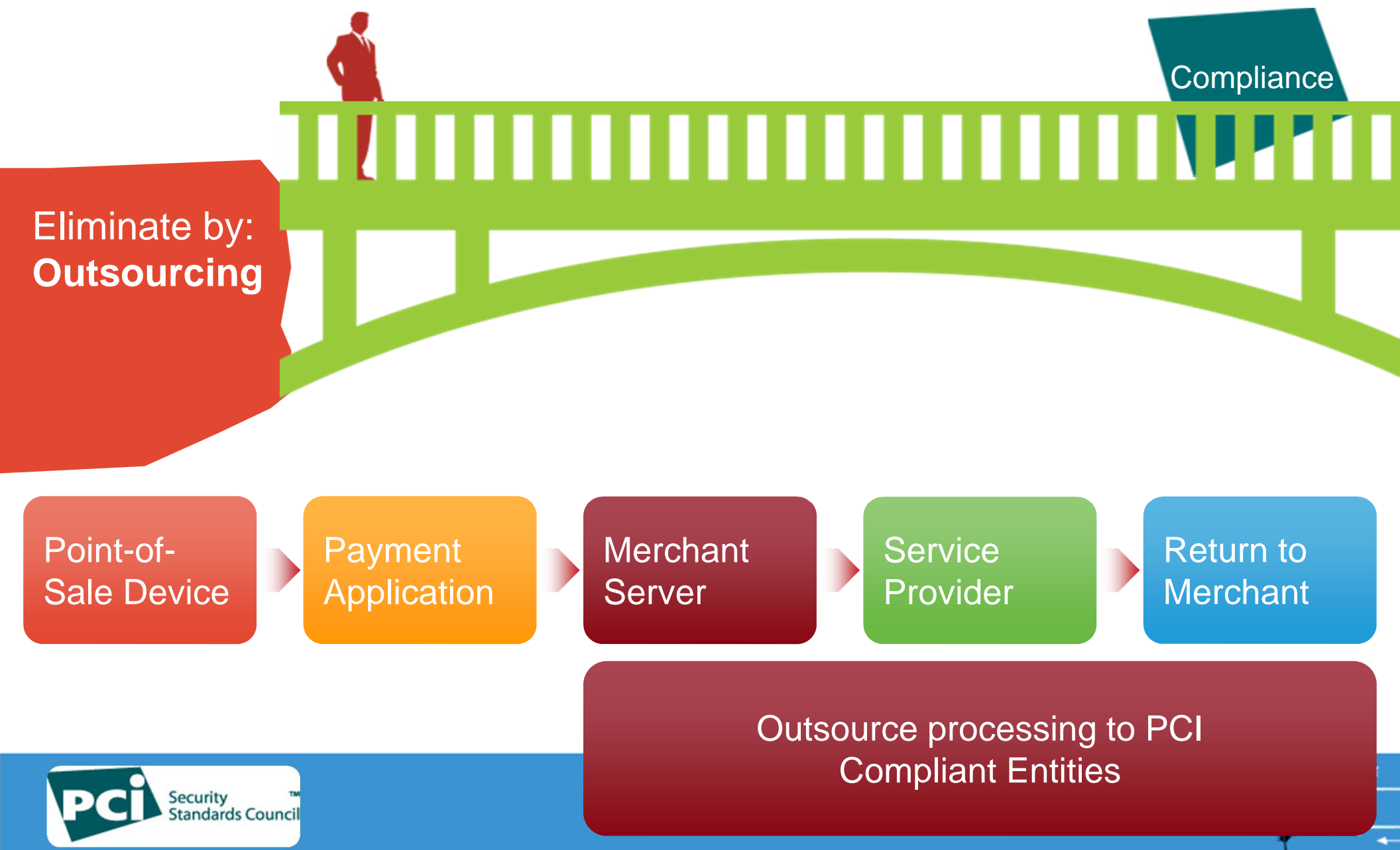
- 1 Creating P2PE requirements
- 2 Providing guidance on tokenization
- 3 Improving the quality of installations
- 4 Updating our training offerings
- 5 Expanding the devices that can be lab tested



PCI Bridge of Compliance



PCI Bridge of Compliance



PCI Bridge of Compliance

Eliminate by:
Outsourcing
Removing

Compliance

Point-of-Sale Device

Payment Application

Service Provider

Return to Merchant

Remove through means such as
TOKENIZATION

PCI Bridge of Compliance

Eliminate by:
Outsourcing
Removing
Encrypting



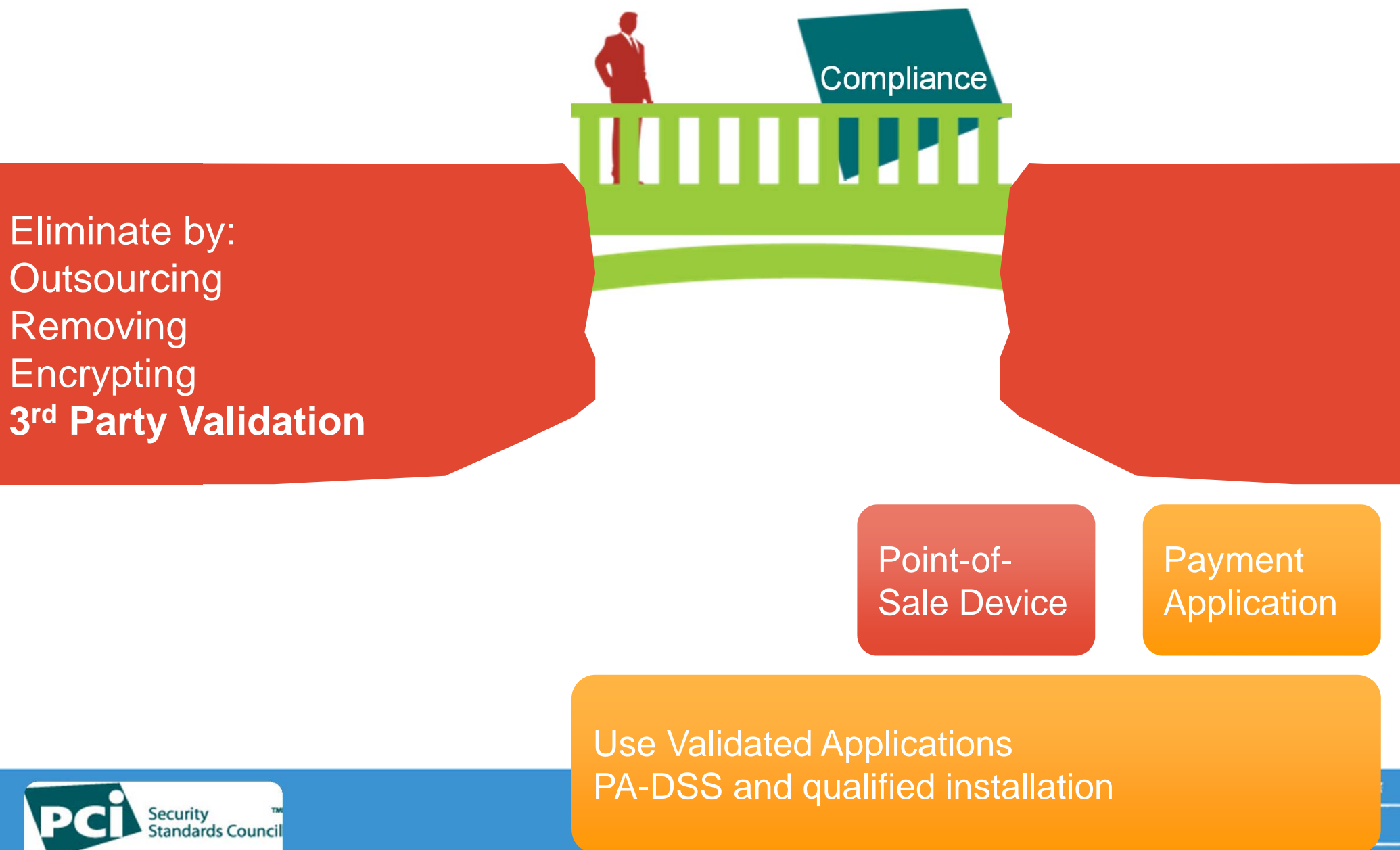
Point-of-Sale Device

Payment Application

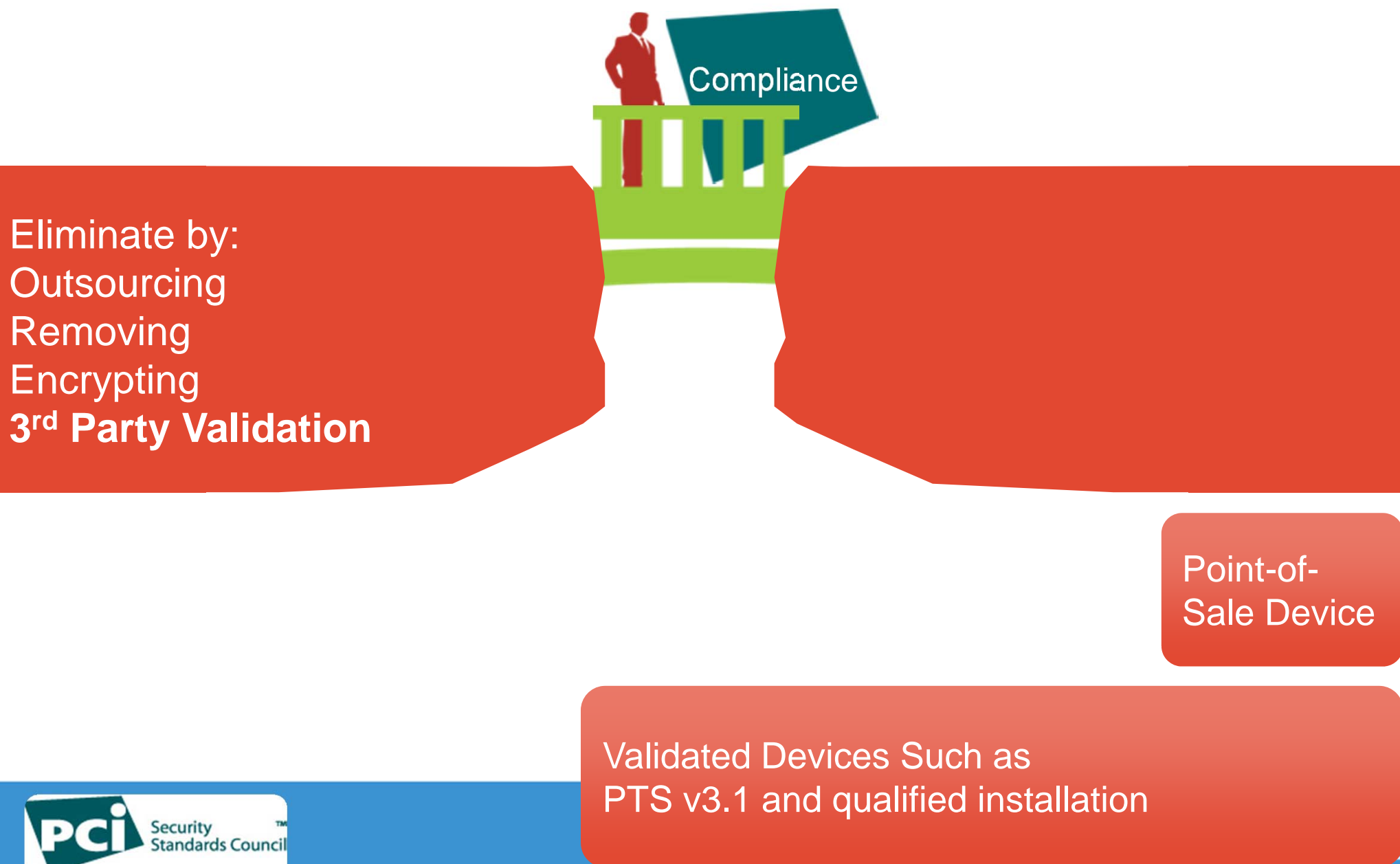
Service Provider

Render Cardholder Data Unreadable Such As P2PE

PCI Bridge of Compliance



PCI Bridge of Compliance





PCI Council Resources

New Guidance - Technologies in Payments



Telephone-based
Payment Card Data



Virtualization



Tokenization



Wireless



EMV



2012 Training Highlights

PCI SSC Internal Security Assessor (ISA) Program

Helps security professionals improve their organizations' understanding of PCI DSS and validate and maintain ongoing compliance



PCI Awareness Training

Offers general PCI training across your business to ensure a universal understanding of PCI compliance

Check out our Training Webinar!

Training Schedule

ISA: Las Vegas, NV, USA – 13-14 April, 2012

QSA: Denver, CO, USA – 1-2 March, 2012

PA-QSA: Orlando, FL, USA – 24-25 February, 2012

PCI Awareness Training online anytime!



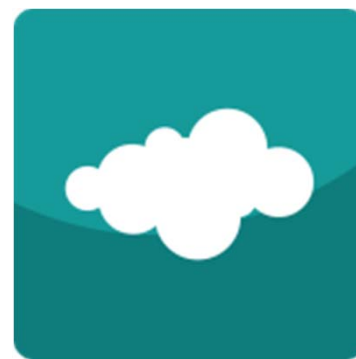
Special Interest Groups (SIGs)



Guidance &
Alignment on
Risk
Assessment



Level 3 and
Level 4 E-
Commerce
Merchants



Cloud
(Virtualization
Phase 2)

sigs@pcisecuritystandards.org

Email today
to join!



Community Meetings

Orlando, Florida

September 12 - 14, 2012



Dublin, Ireland

October 22 - 24, 2012



Join us as a Participating Organization to get involved
in setting global PCI Standards!



Get Involved - Join the PCI Brain trust!



Questions?

