HOSPITALITYLAWYER.COM PRESENTS
THE HOSPITALITY LAW CONFERENCE 2011
FOCUSING ON LEGAL, SAFETY & SECURITY SOLUTIONS
FEBRUARY 9-11, 2011 • HOUSTON, TEXAS

The PCI Security Standards Council

Bob Russo
General Manager, PCI SSC
February 2011

HospitalityLawyer.com

Agenda

- What are the threats to card data?
- How can you defend your card data?
- What is the Council doing to help you?
- What tools are available to get you secure?
- How you can be involved?

What are the threats to card data?

Is this your data?

	Country	Balance	Price
Bank of America (BOA)	USA	...	Sold
Amsouth Bank	USA	$16,040	€700
Washington Mutual Bank (WAMU)	USA	$14,400	€600
Washington Mutual Bank (WAMU)	USA, Multi-Currency Acct.	$7,950 + £2,612	€500
Washington Mutual Bank (WAMU)	USA	...	Sold
MBNA America Bank	USA	$22,003	€1,500
BANCO BRADESCO S.A.	Brazil, Dollar Account	$13,451	€650
CITIBANK	UK, GBP Account	£10,044	€850
NatWest	UK, GBP Account	£12,000	€1000
BNP Paribas Bank	France, Euro Account	€30,792	€2200
Caja de Ahorros de Galocia	Spain, Euro Account	€23,200	€1200
Caja de Ahorros de Galocia	Spain, Euro Account	€7,846	€500
Banc Sabadell	Spain, Euro Account	€25,663	€1450

The Current Threat Landscape

Why SECURITY matters…

"The attackers have changed with the emergence of organized crime into these cybercrimes...It's all about the money now ... Profit is driving these groups." - FBI agent J. Keith Mularski, May 2009

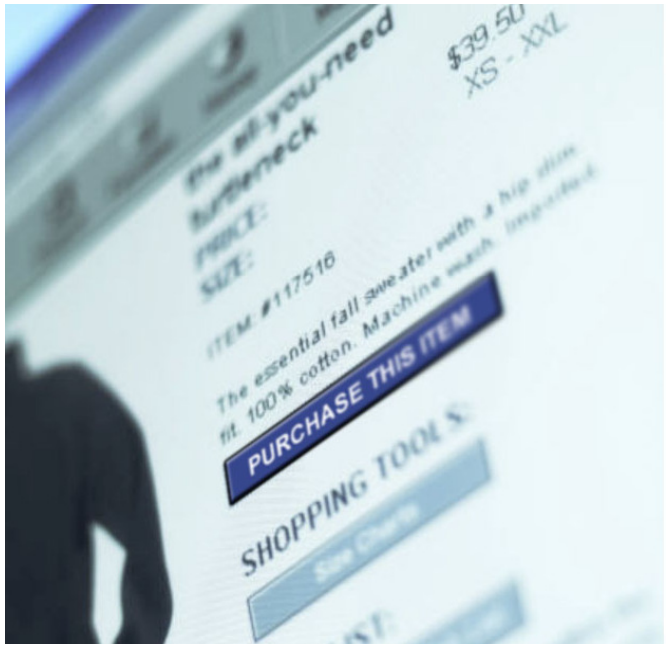
According to Gartner, payment card fraud was the method most actively used by crooks to steal money, claiming 36 percent more victims in 2008 than other types of fraud. - Gartner, March 2009

There were more than 222 million potentially compromised records in 2009 - Identity Theft Resource Center Breach Report, Jan. 8, 2010

"Nearly twice as many people who lost money to fraud in 2008 changed their shopping, payment and e-commerce behavior," said Avivah Litan, vice president and distinguished analyst at Gartner, March 2009

Is your focus on compliance audits rather than security making you a target? Is your risky behavior potentially causing you to lose customers?

Remember, compliance is a byproduct of SECURITY



Forensics Statistics

Inside Jobs vs. Intrusions

51% Inside ~70% were external sources

External breaches make up 98% of records

Internal breaches are now 90% deliberate

89% of records were stolen in targeted attacks

Attack vector (by records)

92% Web Application (SQL injection)

5% backdoor or control channel

2% Remote Access

1% Network Devices

Consumer data:

Payment card information

- Credit / Debit

- Card-present / CNP

Personal Check information

Identity-related data:

Name, address, email

Social security, Social insurance

IRS / tax return information

Company-proprietary:

Financial records

HR / employee data

Product strategy & roadmap

Trade secrets & technology

Time span of Breach Compromise to Discovery

6% - hours

22% - days

24% - weeks

37% - months

7% - years

Over half of the breaches investigated by Verizon in 2009 occurred outside the U.S

The typical breached organization had met just over a third of the requirements of the PCI DSS

HL HospitalityLawyer.com

verizon business

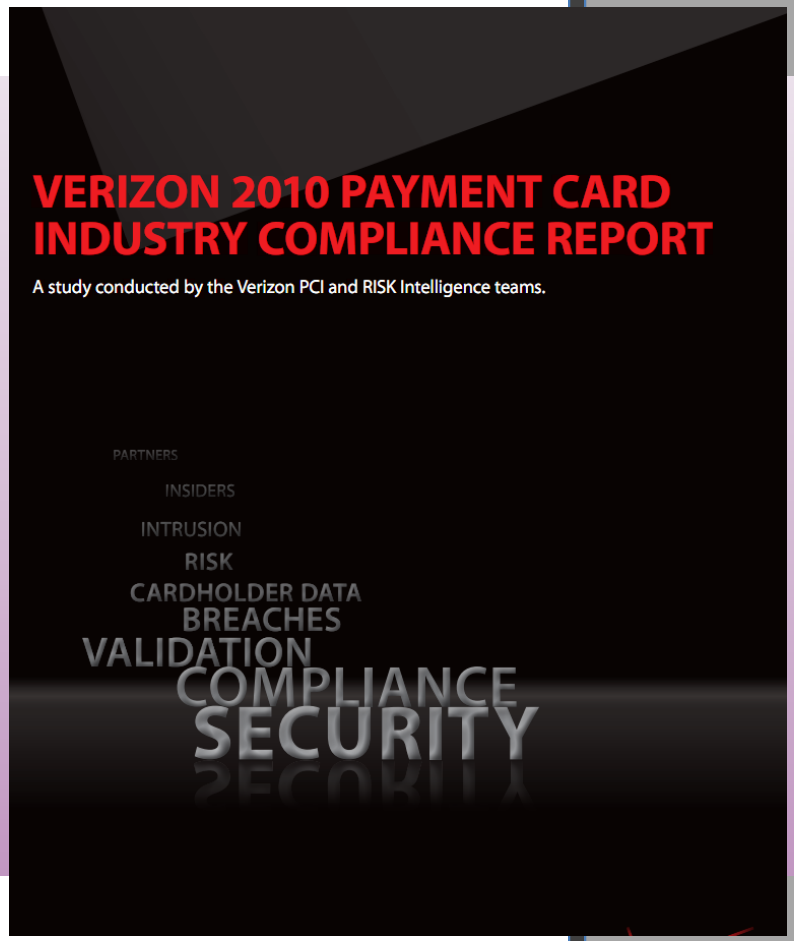
Security Solutions powered by Cybertrust

PCI Specific – Verizon Report

Breached organizations are 50 percent less likely to be PCI-compliant than a "normal population of PCI clients."

Top attack methods used to compromise payment card data:

- malware and hacking (25%)
- SQL injections (24%)
- exploitation of default or guessable credentials (21%)



verizon business
Security Solutions powered by Cybertrust

Risky Behaviors

71% of respondents do not treat PCI as a strategic initiative, yet 79% have experienced a data breach involving the loss or theft of credit card information[1]

More than half (51%) of QSAs say merchants are not proactively managing data privacy and security[2]

73% of respondents have achieved PCI compliance using a basic, checklist approach[2]

55% of respondents focus only on credit card data protection and do not attempt to secure sensitive information[1]

1. PCI DSS Compliance Survey Results - Ponemon Institute Sep. 25, 2009
2. PCI DSS Trends 2010: QSA Insights Report – Ponemon Institute, March 2010

Did You Know?

According to Verizon's 2010 Data Breach Investigations Report (DBIR)

92% of records were compromised through SQL injection

68% of compromises were discovered at least weeks after the compromise

Data security is not all about prevention; it also requires detection and monitoring!

Top Violations

Common Audit / Forensic Results

- Bad or no firewall
- Unprotected stored data
- No security policy
- No unique user IDs
- No tracking or monitoring of access
- No regular tests of security
- Insecure systems and applications

Breaches Cost Money

HospitalityLawyer.com

Value of Compliance

Cost of Complying

- Upgrading payment systems and security
- Verifying compliance via assessment
- Sustaining compliance
- May cost as little as $150 to $2,500 per IP address per year for scans for smaller merchants. Can cost millions for complex or older systems[1]

Cost of a Breach

- "Crisis" upgrades
- Repeat assessments
- Notification
- Brand reputation loss
- Shareholder and consumer lawsuits
- It's estimated that the total cost of a data breach per record is between $90- $300, prior to litigation
- May cost 20 times the price of compliance

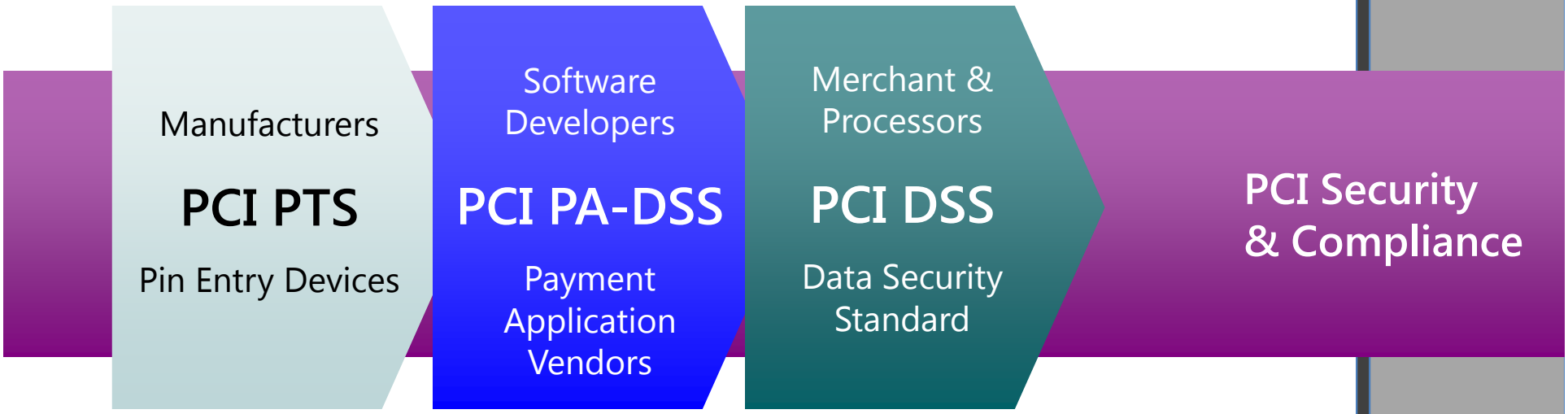
1. PCI Compliance Cost Analysis: A Justified Expense." A joint analysis conducted by Solidcore Systems, Emagined Security and Fortrex. January 2008 \[This study utilized data from several sources including level 1 and level 2 merchants with 2,000 – 2,500 retail locations.]

How can you defend your card data?

PCI Security Standards

Payment Card Industry Security Standards

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

About the Council

Open, global forum

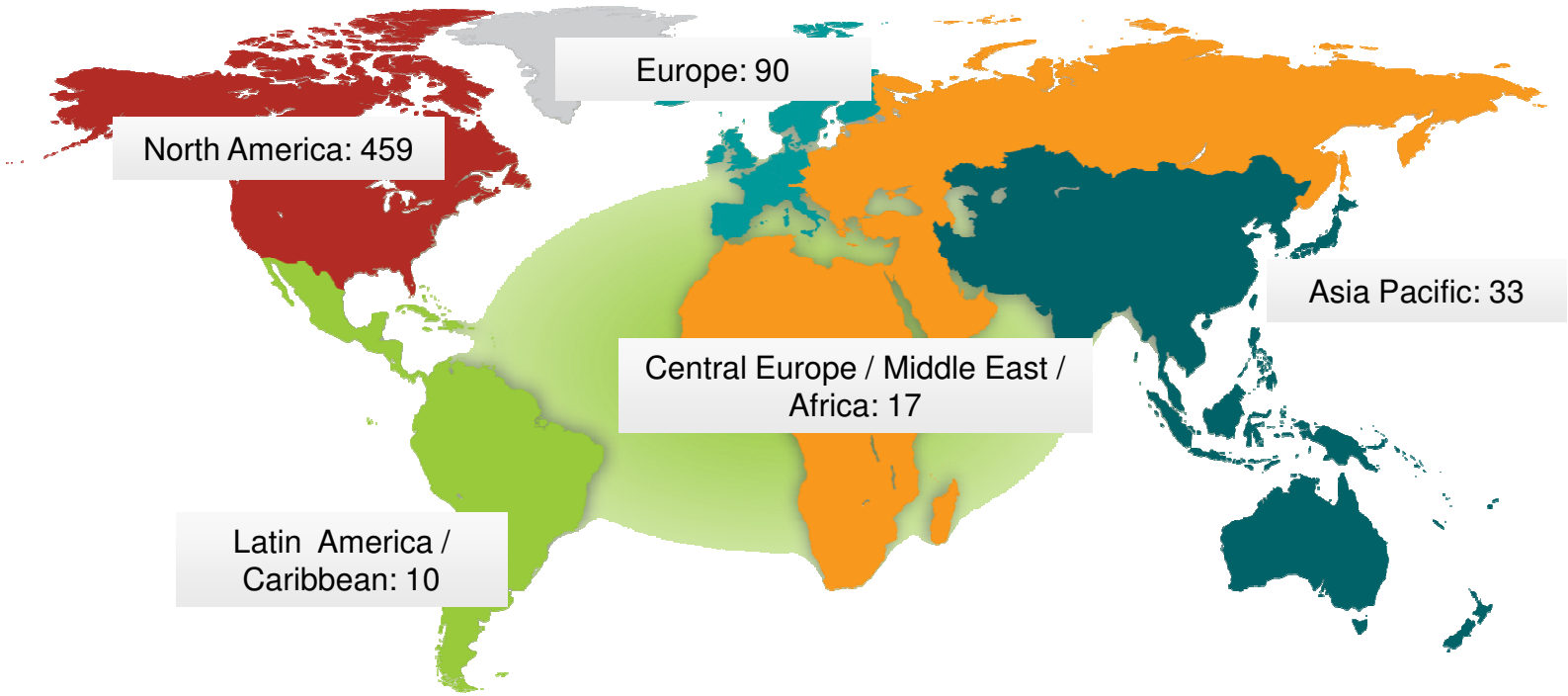
Founded 2006

Responsible for PCI Security Standards

- Development
- Management
- Education
- Awareness

Global Growth

More than 600 organizations have been accepted



Specific Feedback Example

FEEDBACK:

Where elements of cardholder data must be protected when stored in conjunction with PAN, can we get some clarification on what "in-conjunction" means?

Same record, same table, same database, same server, same building, same company?

Clarify Applicability Table in PCI DSS

Technical Working Group:

Updated Applicability Updated table and added text to add clarity

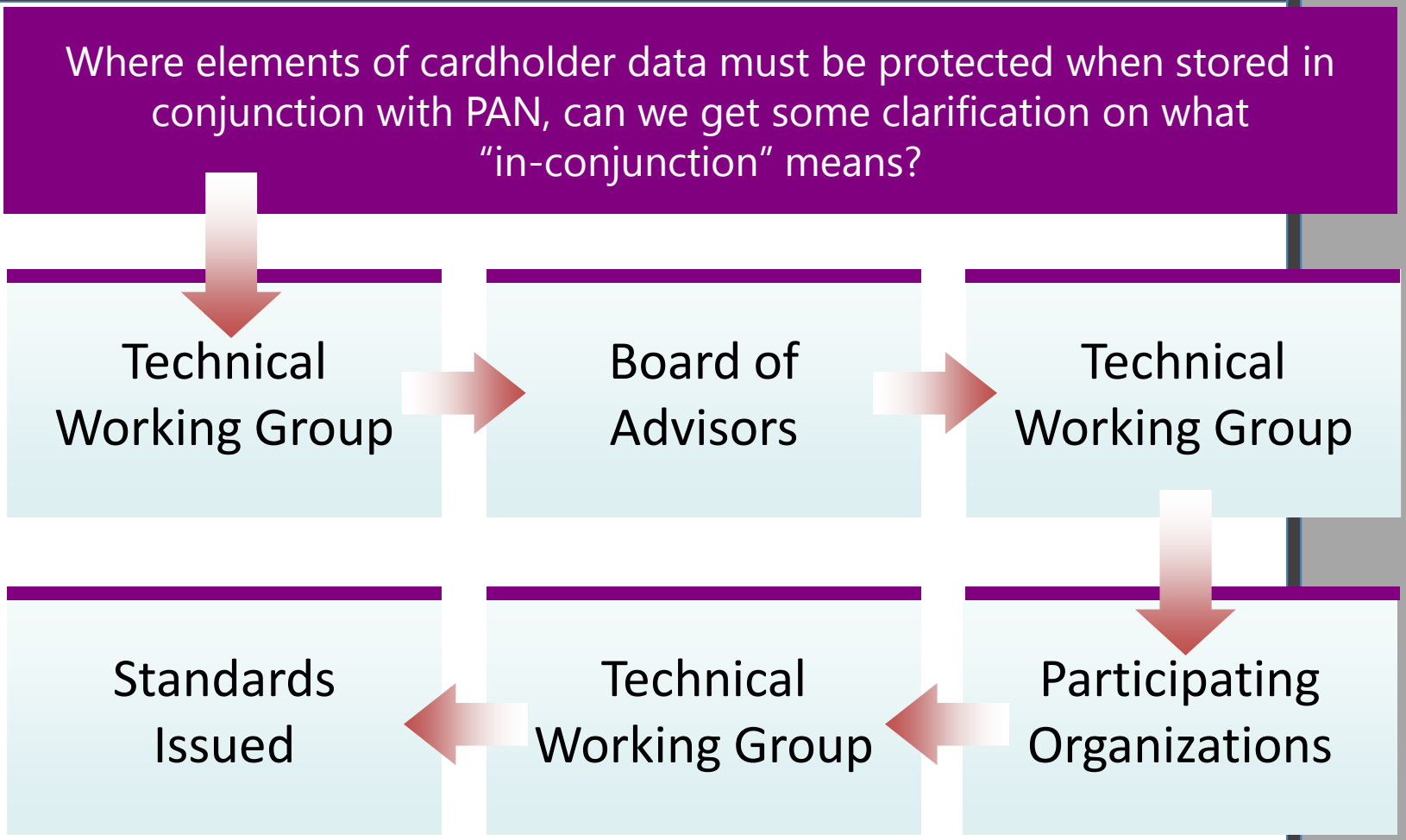
STANDARD CHANGED:

If PAN is stored, processed, or transmitted, AND cardholder name, service code, and/or expiration date is also present in the cardholder data environment, then, per the table below and PCI DSS requirement 3.4, ***only the PAN*** *must be rendered unreadable if stored. All other PCI DSS requirements, EXCEPT 3.3 and 3.4, apply to all cardholder data and the cardholder data environment.*

Legislation additional to PCI DSS, may require specific protection of Personally Identifiable Information (for example, cardholder name), or proper disclosure of a company's practices if consumer-related personal information is being collected during the course of business. Examples include legislation related to consumer personal data protection, privacy, identity theft, or data security.

PCI DSS ***only applies*** *if PANs are stored, processed and/or transmitted.*

How the Process Works

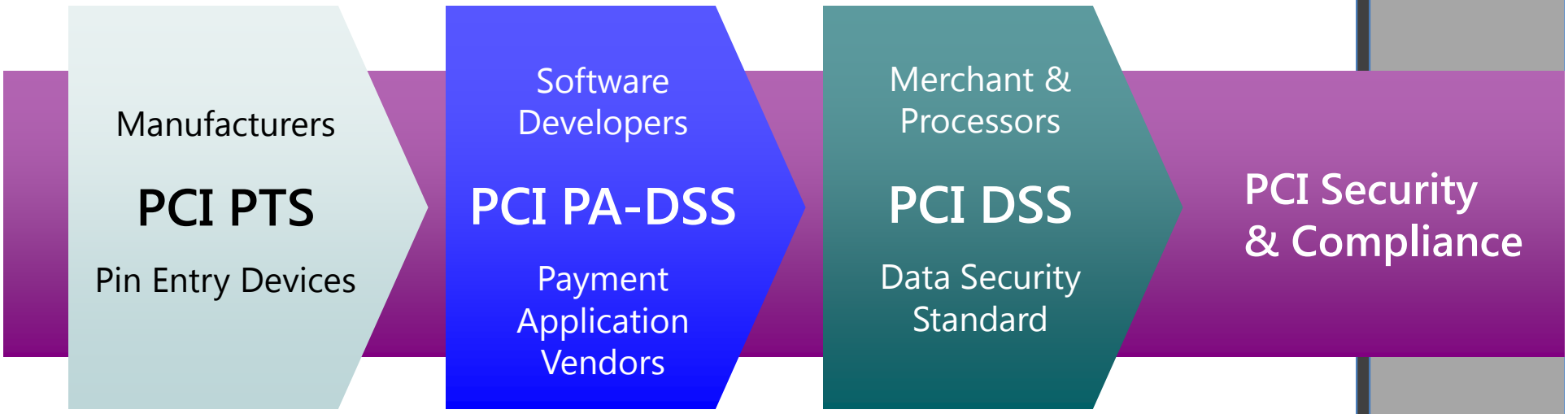


What is the Council doing to help you?

PCI Security Standards

Payment Card Industry Security Standards

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

The Five Stages of Grief

Denial

It doesn't apply to me
PCI compliance is mandatory

de·ni·al

1. ***: refusal to satisfy a request or desire***
2. ***a (1) : refusal to admit the truth or reality (as of a statement or charge) (2) : assertion that an allegation is false b : refusal to acknowledge a person or a thing : disavowal***
3. ***: the opposing by the defendant of an allegation of the opposite party in a lawsuit***

Source: http://www.merriam-webster.com/

The Five Stages of Grief

Anger

It isn't fair

PCI applies to all parties in the payment process

an·ger

transitive verb

: to make angry <he was angered by the decision>

intransitive verb

: to become angry

Source: http://www.merriam-webster.com/

The Five Stages of Grief

Bargaining

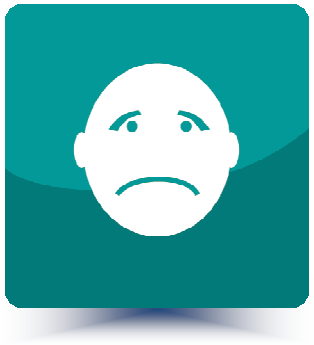
I'll do some of it
Compliance is "pass / fail"

bar·ain·ing

1. ***: an agreement between parties settling what each gives or receives in a transaction between them or what course of action or policy each pursues in respect to the other***
2. ***: something acquired by or as if by bargaining; especially : an advantageous purchase <at that price the car is a bargain>***
3. ***: a transaction, situation, or event regarded in the light of its results <a bad bargain>***

Source: http://www.merriam-webster.com/

The Five Stages of Grief



Depression

I'll never get there
Many merchants already have

de·pres·sion

1. ***(1) : a state of feeling sad : dejection (2) : a psychoneurotic or psychotic disorder marked especially by sadness, inactivity, difficulty in thinking and concentration, a significant increase or decrease in appetite and time spent sleeping, feelings of dejection and hopelessness, and sometimes suicidal tendencies***
2. ***(1) : a reduction in activity, amount, quality, or force (2) : a lowering of vitality or functional activity***

Source: http://www.merriam-webster.com/

The Five Stages of Grief

Acceptance

It'll be OK

PCI doesn't introduce any new, alien concepts

ac·cept·ance

1. : an agreeing either expressly or by conduct to the act or offer of another so that a contract is concluded and the parties become legally bound

Source: http://www.merriam-webster.com/

PCI Data Security Standard

PCI Data Security Standard

Six Goals	Twelve Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

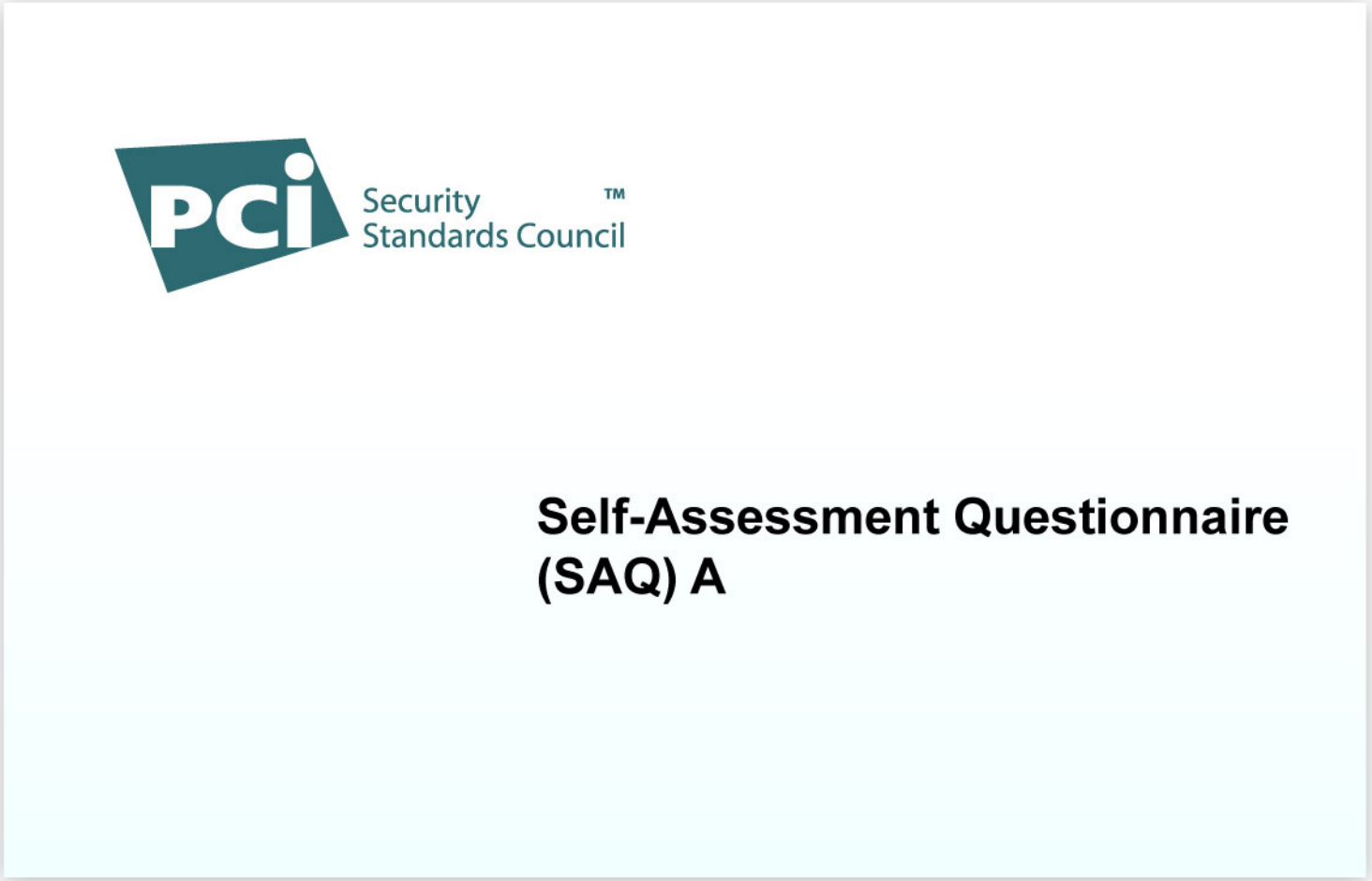
PCI Rock


PCI Data Security Standards Rock
PCICouncil
1 videos
Subscribe
PCI ROCK
"Payment Card Security"
0:05 / 3:45
360p

Payment Application DSS

PIN Transaction Security (PTS)

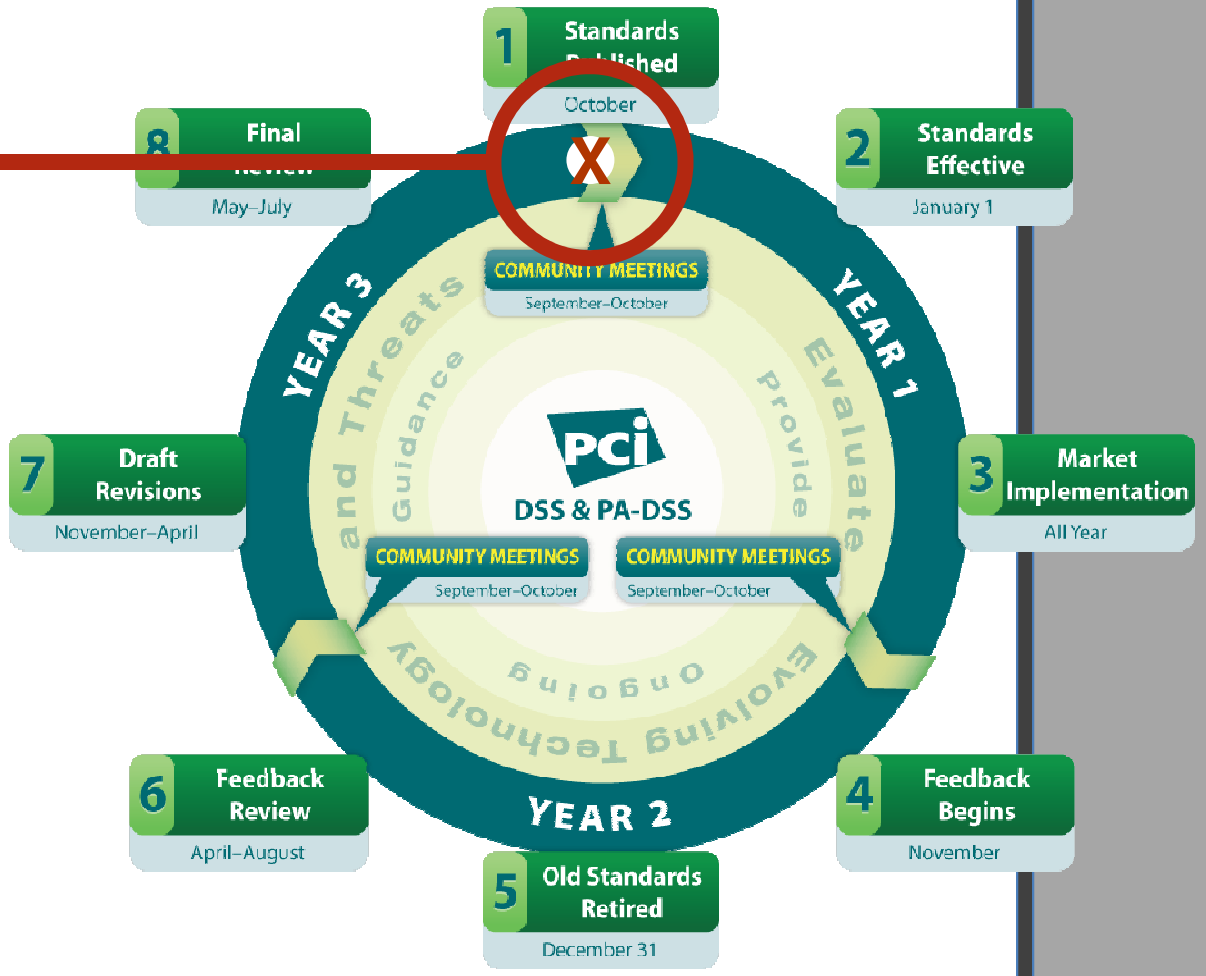
Self-Assessment Questionnaire



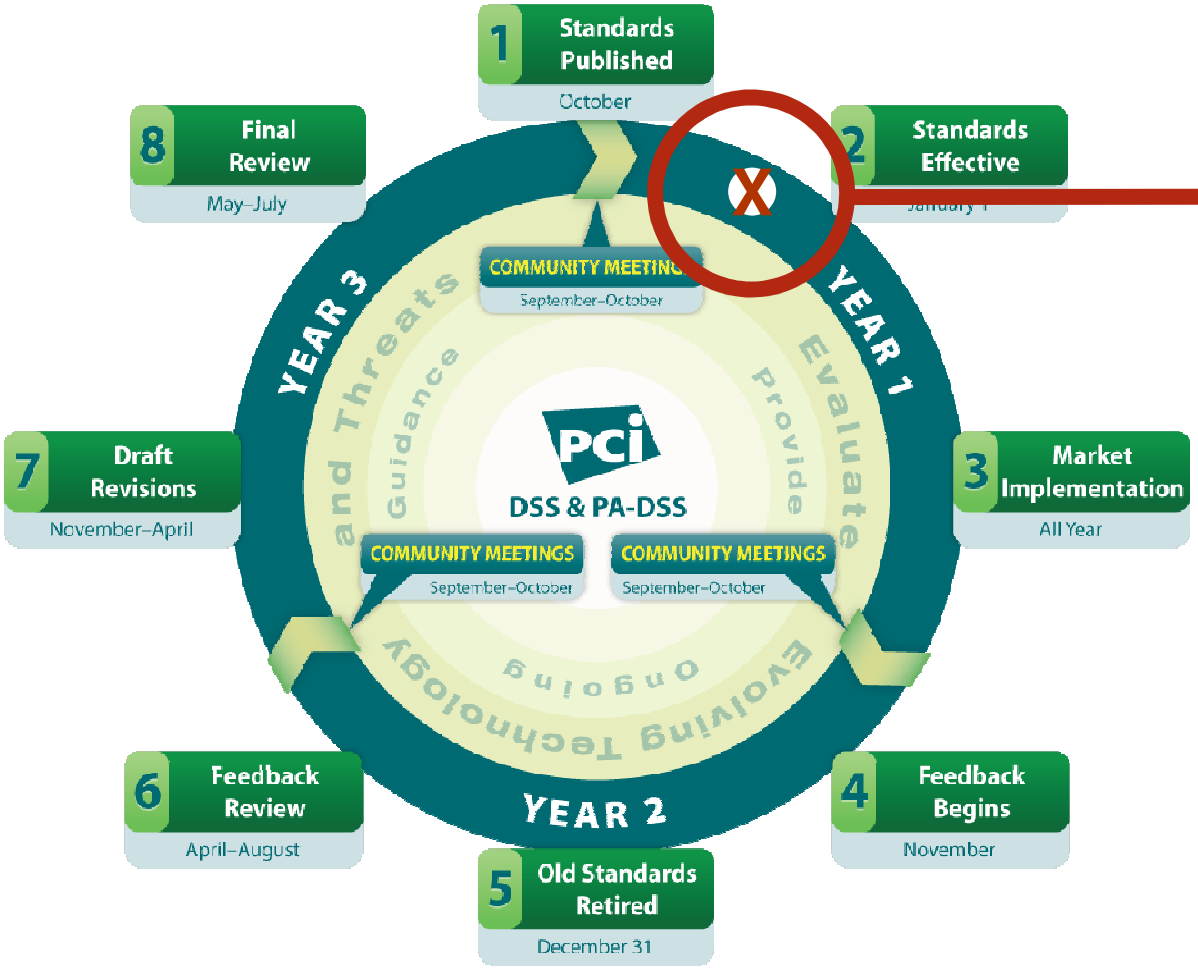
Standards Development Lifecycle

October 2010

Announcement of new standards on October 28, 2010



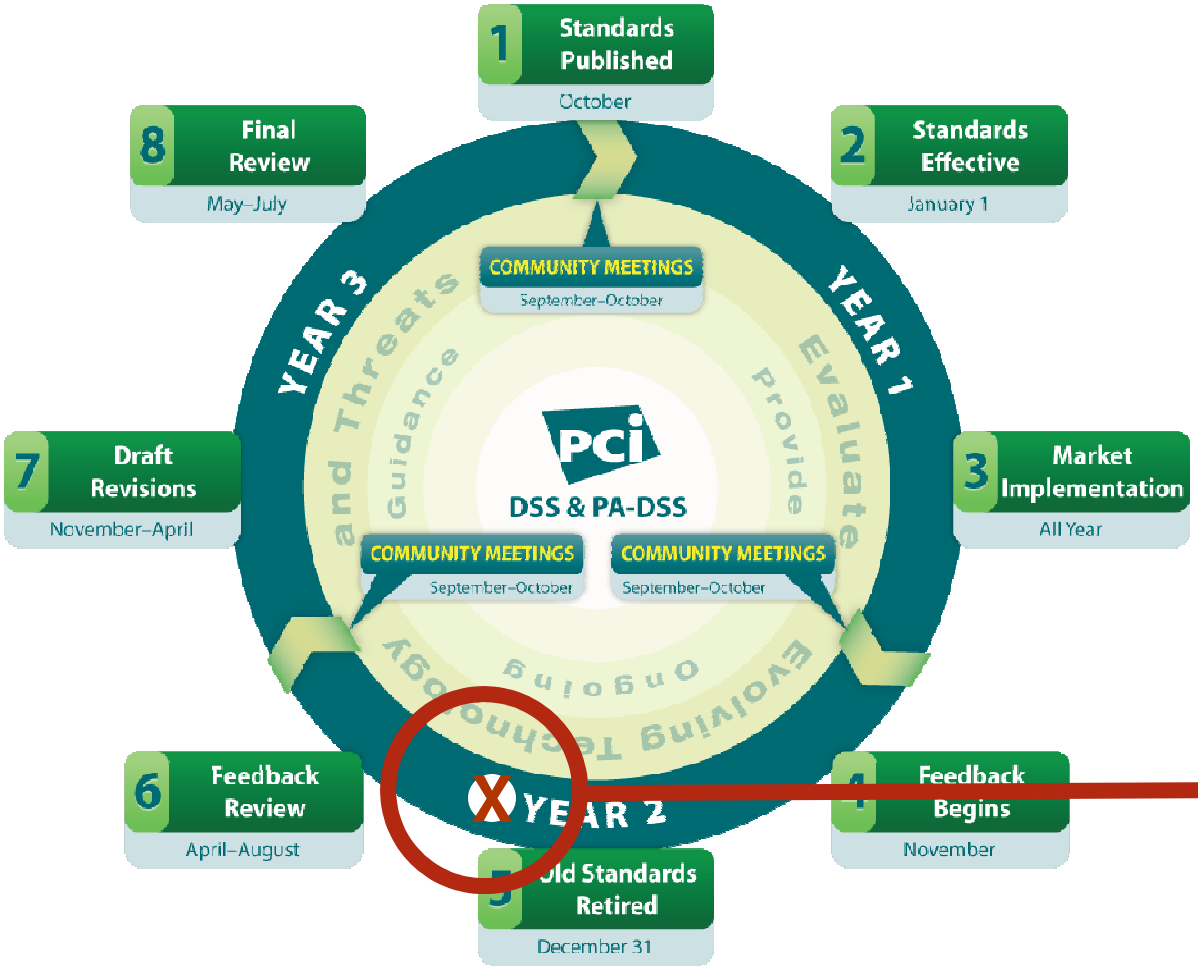
Standards Development Lifecycle



January 2011

New standards effective January 1, 2011

Standards Development Lifecycle



January 2012

All assessments must be completed against DSS 2.0

January 1, 2012

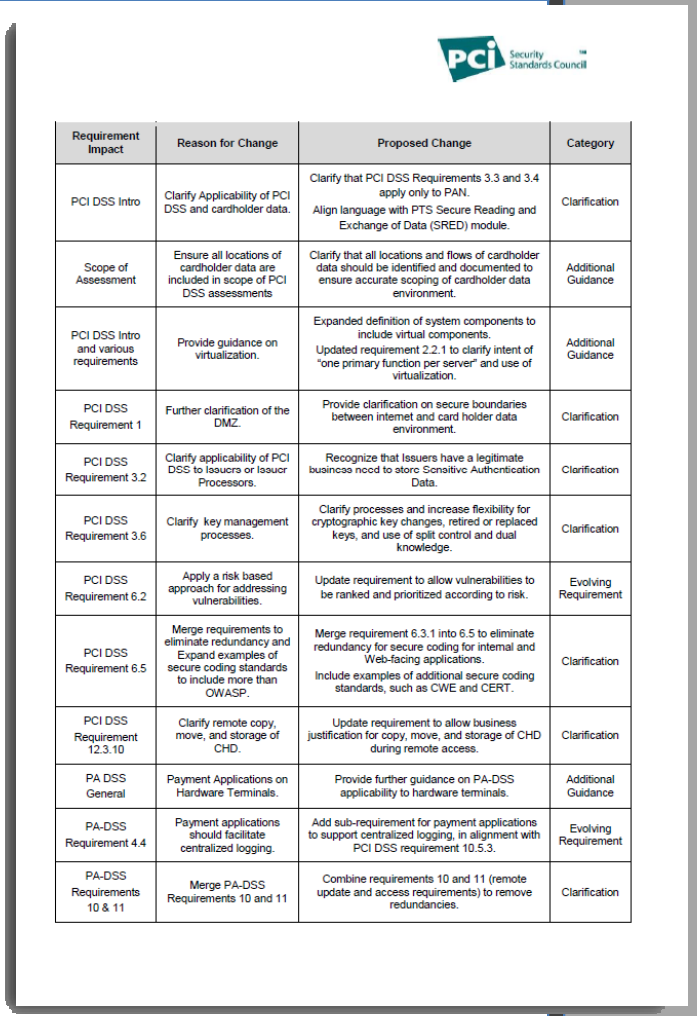
Changes to the DSS and PA-DSS

Clarifications

Additional guidance

Evolving requirements

Your feedback has made the standard more mature and will help secure payment card data well into the future!



Requirement Impact	Reason for Change	Proposed Change	Category
PCI DSS Intro	Clarify Applicability of PCI DSS and cardholder data.	Clarify that PCI DSS Requirements 3.3 and 3.4 apply only to PAN. Align language with PTS Secure Reading and Exchange of Data (SRED) module.	Clarification
Scope of Assessment	Ensure all locations of cardholder data are included in scope of PCI DSS assessments	Clarify that all locations and flows of cardholder data should be identified and documented to ensure accurate scoping of cardholder data environment.	Additional Guidance
PCI DSS Intro and various requirements	Provide guidance on virtualization.	Expanded definition of system components to include virtual components. Updated requirement 2.2.1 to clarify intent of "one primary function per server" and use of virtualization.	Additional Guidance
PCI DSS Requirement 1	Further clarification of the DMZ.	Provide clarification on secure boundaries between internet and card holder data environment.	Clarification
PCI DSS Requirement 3.2	Clarify applicability of PCI DSS to Issuers or Issuer Processors.	Recognize that Issuers have a legitimate business need to store Sensitive Authentication Data.	Clarification
PCI DSS Requirement 3.6	Clarify key management processes.	Clarify processes and increase flexibility for cryptographic key changes, retired or replaced keys, and use of split control and dual knowledge.	Clarification
PCI DSS Requirement 6.2	Apply a risk based approach for addressing vulnerabilities.	Update requirement to allow vulnerabilities to be ranked and prioritized according to risk.	Evolving Requirement
PCI DSS Requirement 6.5	Merge requirements to eliminate redundancy and Expand examples of secure coding standards to include more than OWASP.	Merge requirement 6.3.1 into 6.5 to eliminate redundancy for secure coding for internal and Web-facing applications. Include examples of additional secure coding standards, such as CWE and CERT.	Clarification
PCI DSS Requirement 12.3.10	Clarify remote copy, move, and storage of CHD.	Update requirement to allow business justification for copy, move, and storage of CHD during remote access.	Clarification
PA DSS General	Payment Applications on Hardware Terminals.	Provide further guidance on PA-DSS applicability to hardware terminals.	Additional Guidance
PA-DSS Requirement 4.4	Payment applications should facilitate centralized logging.	Add sub-requirement for payment applications to support centralized logging, in alignment with PCI DSS requirement 10.5.3.	Evolving Requirement
PA-DSS Requirements 10 & 11	Merge PA-DSS Requirements 10 and 11	Combine requirements 10 and 11 (remote update and access requirements) to remove redundancies.	Clarification

At a Glance – Key Updates

- Scoping
- Logging
- Risk-based approach
- Alignment between PA-DSS & PCI-DSS
- Recognition of small merchant environments
- New website and updated supporting documentation

DSS & PA-DSS 2.0 – What's New

- PCI DSS applicability
- Clarify boundaries between the Internet and the CDE (DSS 1.3)
- Issuers and sensitive authentication data (DSS 3.2)

- Rendering PAN unreadable (DSS 3.4)
- Additional sources for secure coding for non-web based applications (DSS 6.5)
- Time synchronization services (DSS 10.4)

DSS & PA-DSS 2.0 – What's New

- Key management procedures (DSS 3.6.4 – 3.6.6)
- Facilitate secure remote software updates (merge PA-DSS 10 & 11)
- More flexible policy for remote access to CHD (12.3.10)

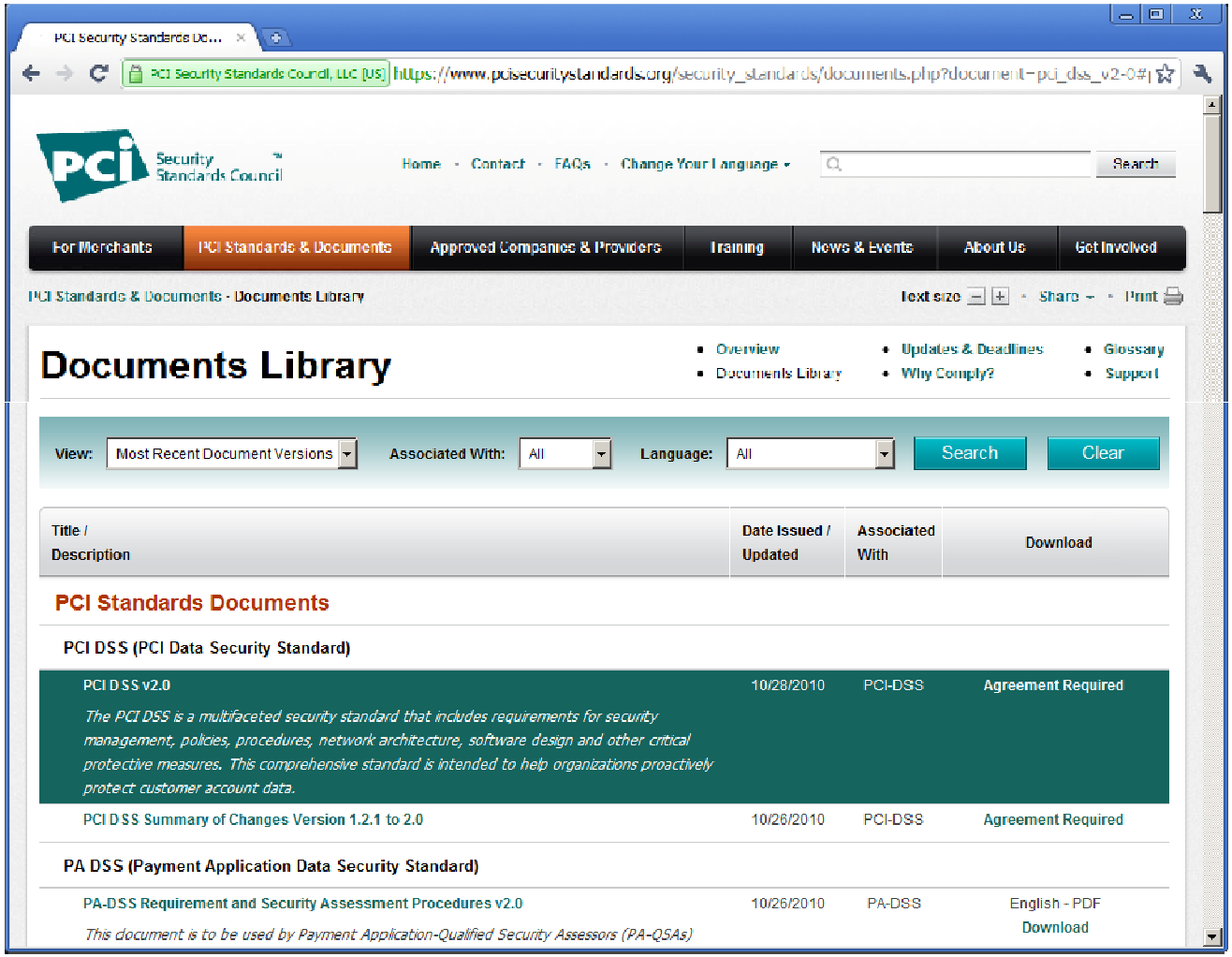
AOCs

- Reformatted for better information flow

SAQs

- Align with new PCI DSS requirements
- Accommodate virtual terminals
- SAQ-C review

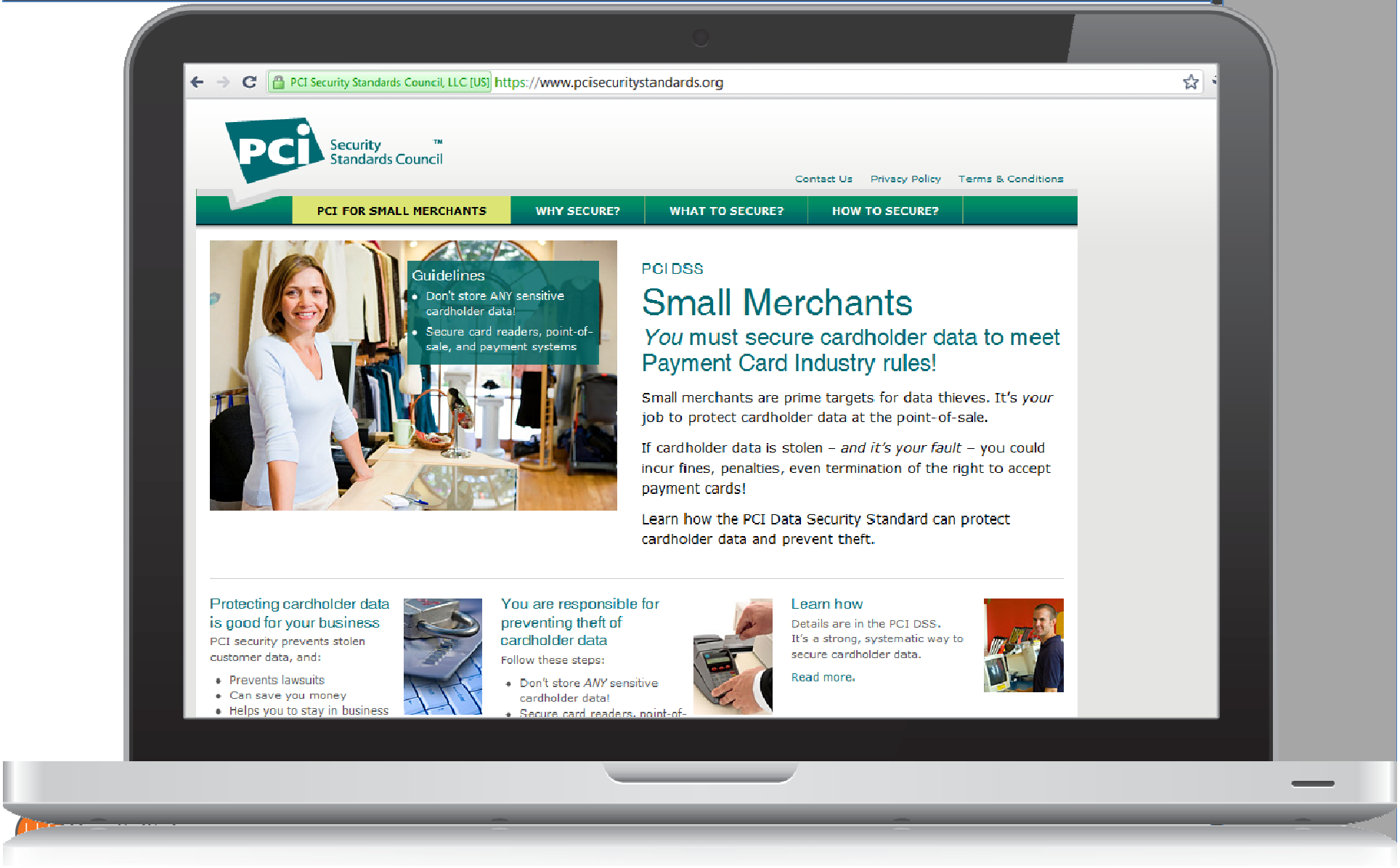
For More Information



What tools are available to get you secure?

Resources for Merchants and Others

Special Resources for Small Merchants



Internal Security Assessor (ISA) Program

PCI SSC Internal Security Assessor Program (ISA)
3-day training and certification course for internal assessment staff

Objective

Test and qualify in-house security personnel on how to validate and maintain ongoing PCI compliance within their organizations

How does this benefit my organization?

- Opportunity to develop internal security expert for driving and maintaining PCI compliance
- Increase internal understanding of PCI standards and controls
- May reduce compliance costs by encouraging development of ongoing security process before and beyond the annual validation

Focus

Improving understanding of PCI standards and compliance through:

- Enhancing the quality, reliability, and consistency of internal PCI-DSS self-assessments
- Supporting the consistent and proper application of PCI-DSS measures and controls
- Effectively facilitating QSA relationships

Internal Security Assessor (ISA) Program

Where?

Feb. 15-16 San Francisco

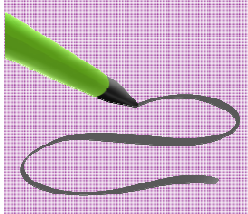
Mar. 9-10 London

Mar. 30-31 Sydney

May San Diego

How much does it cost?

Non-Participating Organization: $2,595
Participating Organization: $1,495



How do I sign up?

Please visit the details in the education section on the website

https://www.pcisecuritystandards.org/education/isa_training.shtml

Difference Between ISA and QSA

Difference	ISA	QSA
Limitation of Validation	Intended only for the Sponsoring Entity and can not validate PA-DSS	Can not validate any entity with which they are invested
Demonstration of experience	Sponsoring Entity attests that the ISA is adequately qualified and receives appropriate training	QSA Company attests to qualifications and provides demonstration of resumes, CPE and background check
Sponsor requirements	Sponsoring Entity must verify criteria and attest Validation Requirements can be met	QSA must attest to Val Req and demonstrate insurance, security firm experience, etc
Quality Assurance	Internal QA program only by the Sponsor	Required internal QA program and SSC sampling

PCI Awareness Training

First PCI SSC Awareness Training

Merchant training endorsed by PCI SSC

Objective

Arm merchants with everything they need to know to best prepare for an onsite PCI DSS inspection or to perform the assessment internally

Where

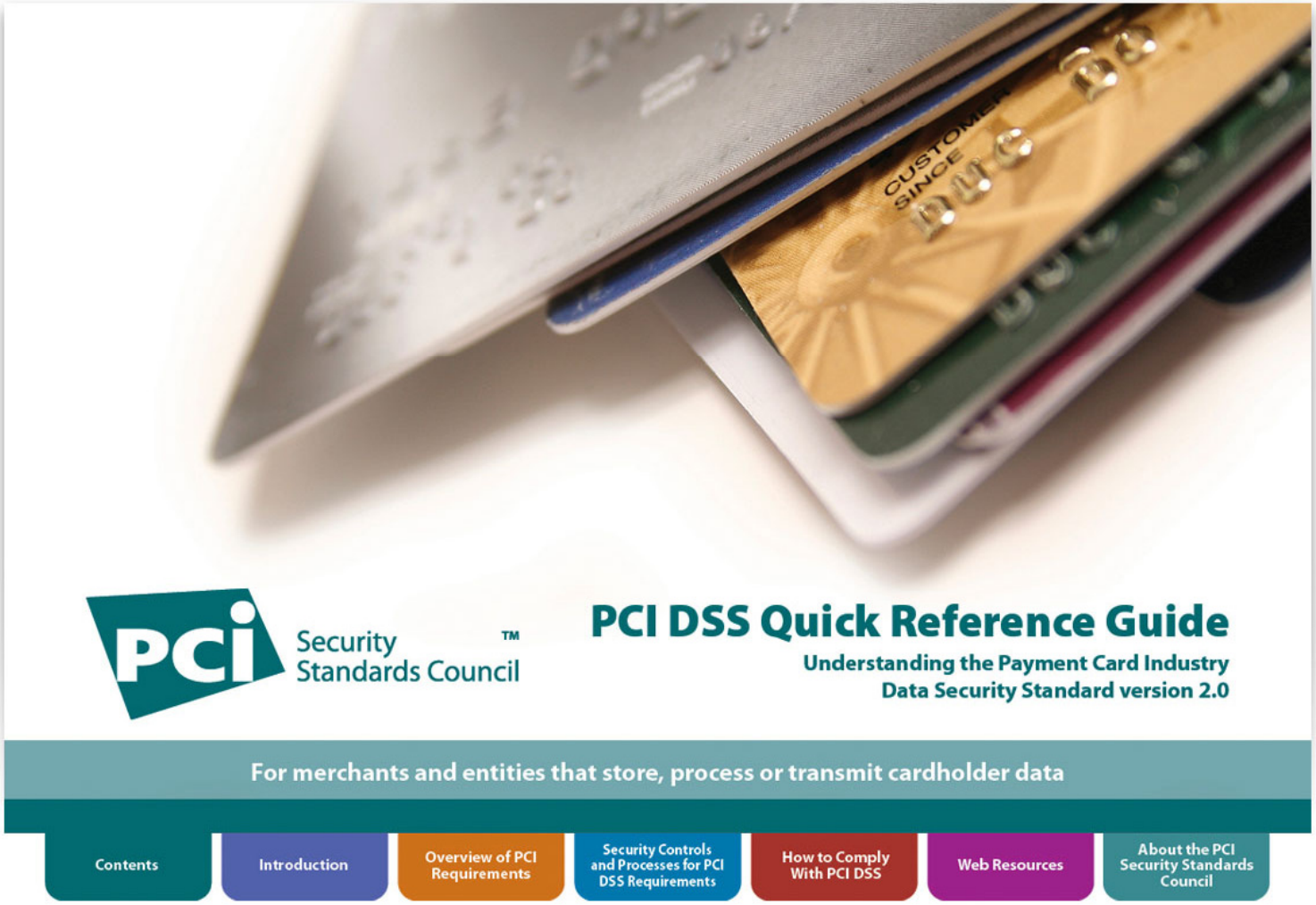
- Locations in 2010
- Please visit the Council's Training website for an up to date schedule of courses and registration details

Focus

Four key modules

- PCI Program – defining the payment card industry
- Scoping a PCI DSS Assessment
- PCI DSS v2.0 Requirements
- Compensating Controls

PCI Quick Reference Guide



HL HospitalityLawyer.com

PCI DSS Prioritized Approach

PCI Security Standards Council

PCI DSS PRIORITIZED APPROACH

PCI COMPLIANCE IS A CONTINUOUS PROCESS

ASSESS

REPORT

REMEDIATE

PCI SSC FOUNDERS

PARTICIPATING ORGANIZATIONS

Merchants, banks, processors, developers and point of sale vendors

Disclaimer

To achieve PCI DSS compliance, an organization must meet all PCI DSS requirements, regardless of the order in which they are satisfied or whether the organization seeking compliance follows the PCI DSS Prioritized Approach. This document does not modify or abridge the PCI DSS or any of its requirements, and may be changed without notice. PCI SSC is not responsible for errors or damages of any kind resulting from the use of the information contained herein. PCI SSC makes no warranty, guarantee, or representation as to the accuracy or sufficiency of the information provided herein, and assumes no responsibility or liability regarding the use or misuse of such information.

Milestones for Prioritizing PCI DSS Compliance Efforts

The Prioritized Approach includes six milestones. The matrix below summarizes the high-level goals and intentions of each milestone. The rest of this document maps the milestones to each of all twelve PCI DSS requirements and their sub-requirements.

Milestone	Goals
1	**Remove sensitive authentication data and limit data retention.** This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it.
2	**Protect the perimeter, internal, and wireless networks.** This milestone targets controls for points of access to most compromises – the network or a wireless access point.
3	**Secure payment card applications.** This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.
4	**Monitor and control access to your systems.** Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment.
5	**Protect stored cardholder data.** For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data.
6	**Finalize all policies, procedures, and processes to support maintenance of PCI DSS compliance.** The intent of Milestone 6 is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment. The milestone also includes completion of firewall configuration standards, change control procedures, securing audit trails, and network testing processes.

Prioritized Approach Tools

PCI DSS Requirements		Milestone					
		1	2	3	4	5	6
Requirement 1: Install and maintain a firewall configuration to protect cardholder data							
1.1	Establish firewall and router configuration standards that include the following:						6
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations						6
1.1.2	Current network diagram with all connections to cardholder data, including any wireless networks	1					
1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone		2				
1.1.4	Description of groups, roles, and responsibilities for logical management of network components						6
1.1.5	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure		2				
1.1.6	Requirement to review firewall and router rule sets at least every six months						6
1.2	Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.		2				
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.						

Board of Advisors Election

Join as a Participating Organization by going to
https://www.pcisecuritystandards.org/get_involved/join.php
and play a role in electing the next Board of Advisors

Community Meetings

Two Meetings in 2011:

Scottsdale, AZ
September 20 – 22, 2011

Europe, TBD
October 24 – 26, 2011

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

Fact Sheets

PCI Security Standards Council

Lifecycle for Ch

The Payment Card Industry PI
Security (PTS) requirements ar
primarily by point-of-sale equi
manufacturers to secure cardh
at the physical point of sale. T
is managed by the PCI Securit
Council (PCI SSC). Input for pr
changes to the standard are a
by PCI SSC stakeholders – Pa
Organizations, including merch
banks, processors, hardware a
developers, point-of-sale vend
approved security evaluation l

Changes to the standard follow
36-month lifecycle with eight s
described below. The lifecycle
gradual, phased use of new ve
standard without invalidating c
noncompliant when changes a
Throughout the lifecycle, the C
ongoing guidance about these

NEW STANDARD PUBLISHED

- Major new release of PTS
- Presented at Community Meetings in October
- Initiates 3-year lifecycle
- Previous version remains effective for 12 months after the new standard becomes effective

PCI Security Standards Council

Overview of the Information Supp

The near ubiquity of wireless n
a top priority for organizations
or transmit cardholder data. In
Security Standards Council Sp
Implementation Team has pub
supplement called PCI DSS W
The goal of this document is t
understand how PCI DSS appl
environments, how to limit the
pertains to wireless, and provi
and concepts for deployment
in payment card transaction er
also intended for assessors wh
compliance. This At-a-Glance
32-page Guideline.

HIGHLIGHTS

- Provides guidance for testing or deploying 802.11 Wireless Local Area Networks (WLAN)
- Focuses on suggestions for deploying WLAN in the Cardholder Data Environment
- Includes operational procedures required to make WLAN part of a PCI DSS compliant network

PCI Security Standards Council

Skimming Preven
Overview of Best

Skimming is the unauthorized captur
of payment data to another source. I
to commit fraud, the threat is seriou
any merchant's environment. With sk
steal payment data directly from the
payment card or from the payment i
merchant location. Both techniques
the use of a rogue physical device pl
PCI Security Standards currently cor
requirements and recommendations
skimming. In addition, the Council ha
overview document for merchants c
dive" about skimming, examples, be
tools to thwart its use. This "At-a-Gla
snapshot of skimming and introduce
countermeasures to ensure an appro
security for cardholder data.

HIGHLIGHTS

Describes the problem of skimming with several examples of actual gear used to steal cardholder data

Provides best practices to mitigate the risk of skimming

Includes written methodology to quantify risk of skimming and a checklist for tracking assets in a specific merchant location and terminal environment

PCI Security Standards Council

AT A GLANCE
PCI DATA STORAGE

PCI Data Storage Do's and Don'ts

Requirement 3 of the Payment Card Industry's Data Security Standard (PCI DSS) is to "protect stored cardholder data." The public assumes merchants and financial institutions will protect data on payment cards to thwart theft and prevent unauthorized use. But merchants should take note: Requirement 3 applies only if cardholder data is stored. Merchants who do not store any cardholder data automatically provide stronger protection by having eliminated a key target for data thieves.
For merchants who have a legitimate business reason to store cardholder data, it is important to understand what data elements PCI DSS allows them to store and what measures they must take to protect those data. To prevent unauthorized storage, only Council certified PIN entry devices and payment applications may be used. PCI DSS compliance is enforced by the major payment card brands who established the PCI DSS and the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI SSC FOUNDERS

PARTICIPATING ORGANIZATIONS

Merchants, Banks, Processors, Hardware and Software Developers and Point-of-Sale Vendors

Basic PCI Data Storage Guidelines for Merchants

Cardholder data refers to any information contained on a customer's payment card. The data is printed on either side of the card and is contained in digital format on the magnetic stripe embedded in the backside of the card. Some payment cards store data in chips embedded on the front side. The front side usually has the primary account number (PAN), cardholder name and expiration date. The magnetic stripe or chip holds these plus other sensitive data for authentication and authorization.
In general, no payment card data should ever be stored by a merchant unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored. Only the PAN, expiration date, service code, or cardholder name may be stored, and merchants must use technical precautions for safe storage (see back of this fact sheet for a summary). The matrix below shows basic "do's" and "don'ts" for data storage security.

Data Do's	Data Don'ts
Do understand where payment card data flows for the entire transaction process	Do not store cardholder data unless it's absolutely necessary
Do verify that your payment card terminals comply with the PCI personal identification number (PIN) entry device (PED) security requirements	Do not store sensitive authentication data contained in the payment card's storage chip or full magnetic stripe, including the printed 3-4 digit card validation code on the front or back of the payment card after authorization
Do verify that your payment applications comply with the Payment Application Data Security Standard (PA-DSS)	Do not have PED terminals print out personally identifiable payment card data; printouts should be truncated or masked
Do retain (if you have a legitimate business need) cardholder data only if authorized, and ensure it's protected	Do not store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones
Do use strong cryptography to render unreadable cardholder data that you store, and use other layered security technologies to minimize the risk of exploits by criminals	Do not locate servers or other payment card system storage devices outside of a locked, fully-secured and access-controlled room
Do ensure that third parties who process your customers' payment cards comply with PCI DSS, PED and/or PA-DSS as applicable. Have clear access and password protection policies	Do not permit any unauthorized people to access stored cardholder data

Additional Guidance on Technologies in Payments

Continue to look for guidance from the Council on emerging technologies

These supplements produced by the Council will help you better understand how the implementation of specific technologies define or reshape the cardholder data environment

Technologies in Payments

Tokenization

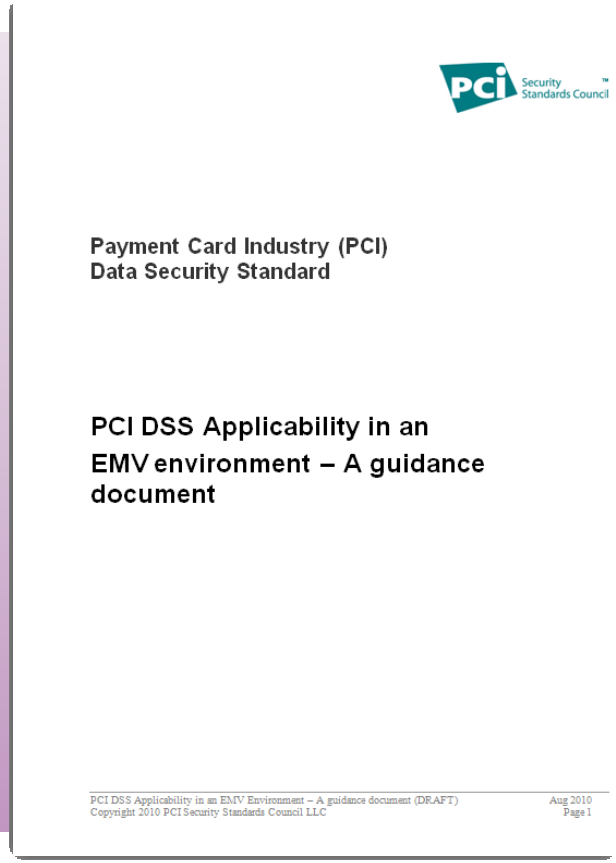
Encryption

Wireless

EMV

Virtualization

Technologies in Payments: EMV



The guidance document provides background information for organizations that are considering implementations of EMV technology within the context of PCI DSS compliance.

Technologies in Payments

The Council is committed to an ongoing assessment of technologies in payments

- EMV and P2P guidance are a first step
- Reflects your input and industry collaboration
- Evaluates the impact of these technologies on PCI DSS compliance efforts
- Reinforces the effectiveness of PCI DSS as a strong method for protecting cardholder data

There is more work to be done
– and we need your continued feedback and participation!

Council Resources

Security standards and supporting documents

Quick Reference Guide

Searchable Frequently Asked Questions

List of approved QSAs, ASVs, PA-QSAs, PED Labs

Education and outreach - e.g., fact sheets, webinars

Participating membership, meetings, collaboration

A global voice for the industry

HOSPITALITYLAWYER.COM PRESENTS

THE 2011 HOSPITALITY LAW CONFERENCE

FOCUSING ON LEGAL, SAFETY & SECURITY SOLUTIONS

FEBRUARY 9-11, 2011 • HOUSTON, TEXAS

How can you be involved?

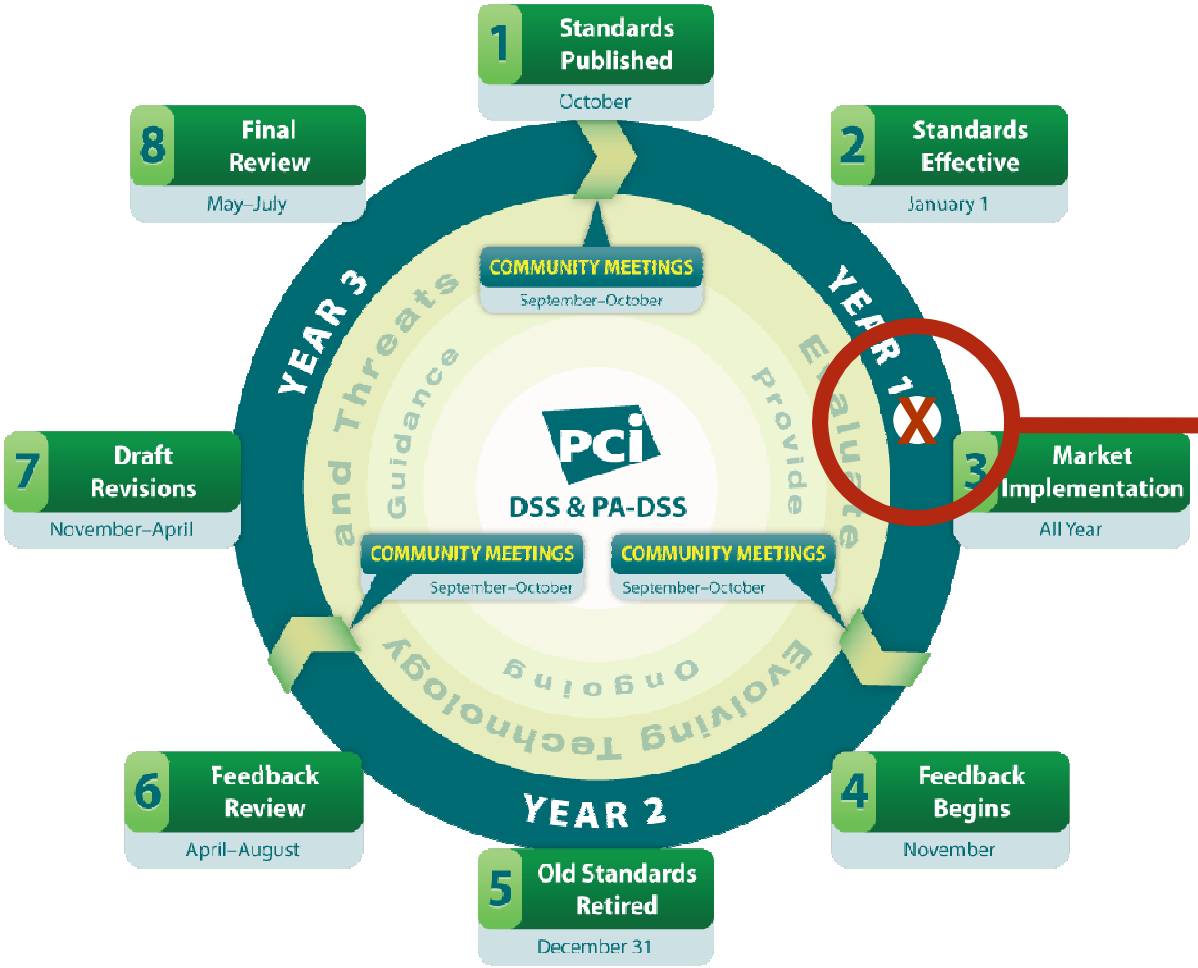
HospitalityLawyer.com

We Welcome Your Involvement

Get Involved

PCI security landscape and standards are maturing globally

Provide Feedback to the Council



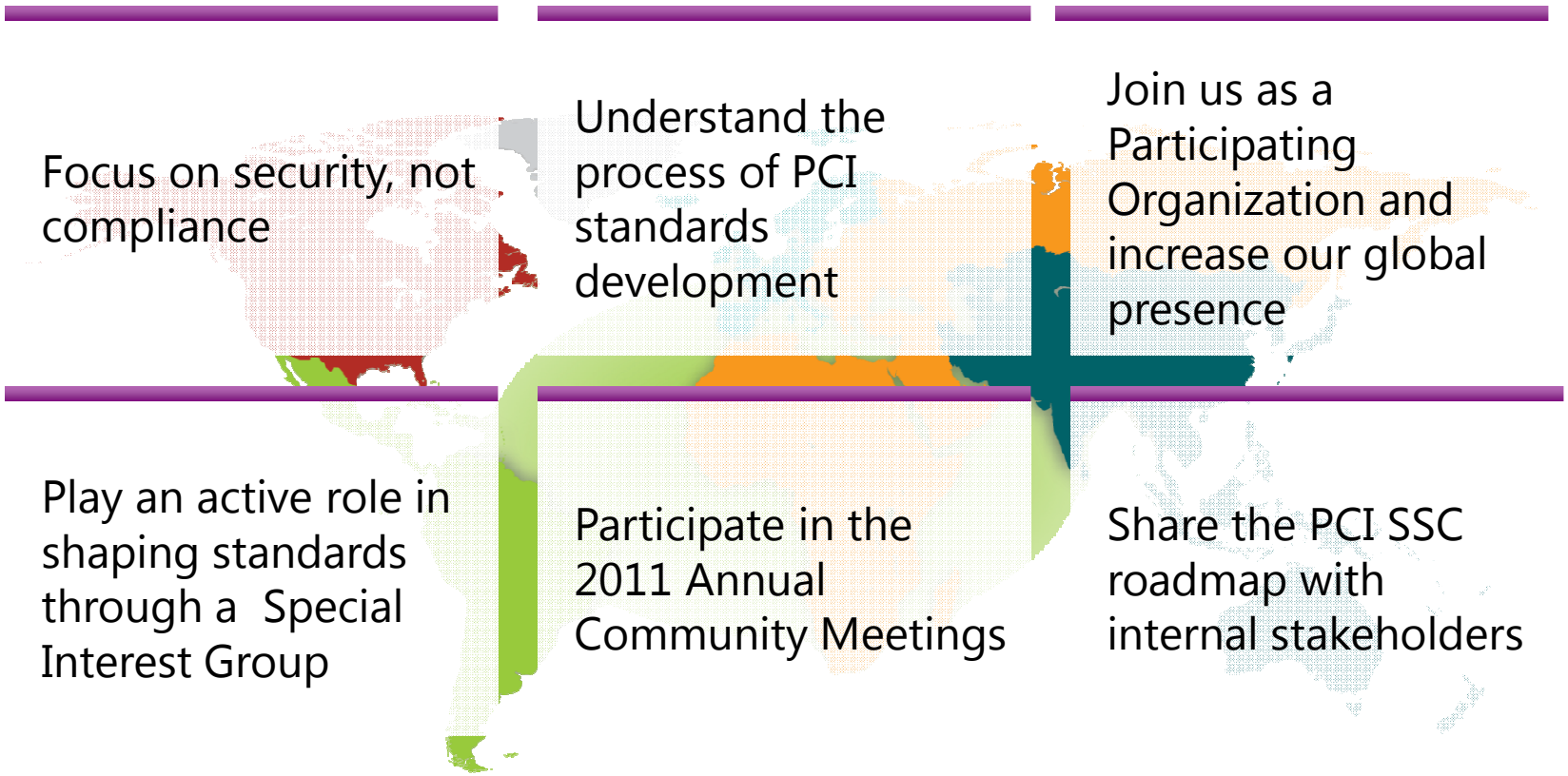
Feedback on newest standards

Special Interest Groups

What do Special Interest Groups do?

- Opportunity to leverage Participating Organizations' expertise
- SIGs analyze and address specific industry challenges
- SIGs determine own deliverables
- Recommend changes, clarifications, improvements, best practices, etc.
- Work with Board of Advisor Leader to channel info into the SSC
- SIGs dissolve after deliverable is achieved
- New SIGs can be proposed at any time

Summary



Focus on security, not compliance

Understand the process of PCI standards development

Join us as a Participating Organization and increase our global presence

Play an active role in shaping standards through a Special Interest Group

Participate in the 2011 Annual Community Meetings

Share the PCI SSC roadmap with internal stakeholders

Security is Only as Good as the Weakest Link

Stay Involved

Even though you have more time, move toward adopting 2.0 ASAP

Take advantage of the Council's resources and guidance

Participate in a SIG

Keep Sending Us Your Feedback!