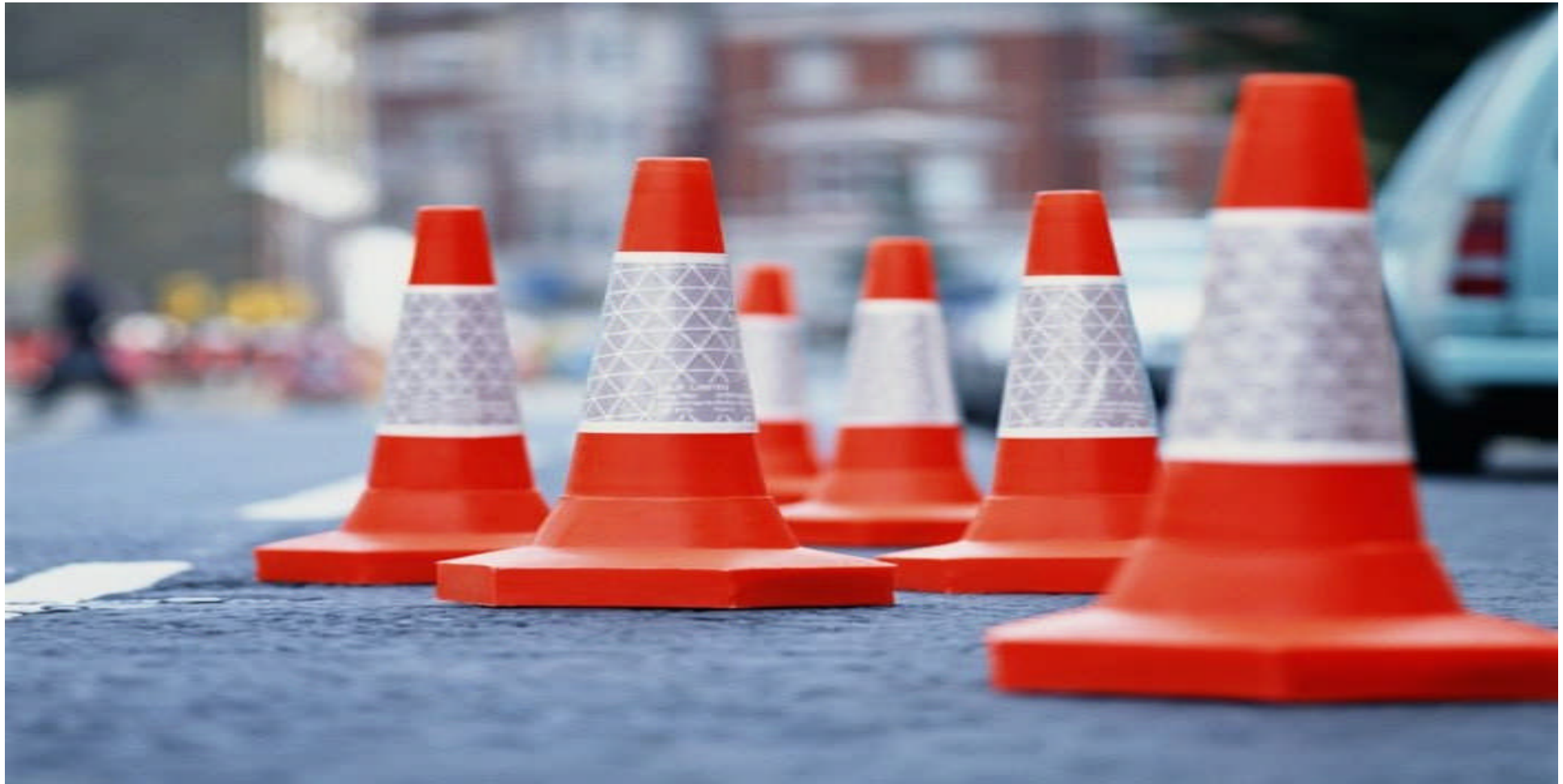


Compliance with the PCI Data Security Standard

ISACA Nashville Training Day

November 2009



Agenda

- Introduction
- PCI Overview
- Leading Practices and Challenges
- Our Capabilities and Experience
- Q&A

About PricewaterhouseCoopers

PricewaterhouseCoopers (www.pwc.com) provides industry-focused assurance, tax and advisory services to build public trust and enhance value for its clients and their stakeholders. More than 154,000 people in 153 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

About PricewaterhouseCoopers' Advisory Practice

PricewaterhouseCoopers' business advisory professionals provide clients with the confidence to succeed by helping them anticipate, create and manage change. Whether clients are proactively implementing change or reacting to an unplanned event, we leverage our network's resources, deep industry experience, and functional acumen across the areas of operations, finance, organizational strategy and structure, process improvement, human resources effectiveness, technology integration and implementation, risk mitigation and crisis management to help organizations effect sustainable change.

Overview of the PCI Data Security Standard

- The Payment Card Industry Data Security Standard (PCI DSS) was **developed by the card brands** in response to the alarming increase in payment card theft and fraud
- Due to **anti-trust regulations**, each of the 5 major card brands have their own PCI compliance program that leverages the PCI DSS as the underlying controls framework
- All companies that **process, store or transmit** payment card data (regardless of merchant or service provider level) have to be compliant with the PCI DSS
- The PCI DSS has been endorsed by the major credit card brands and is overseen by the independent legal entity called the **PCI Security Standards Council (SSC)**
- The PCI DSS contains **12 requirements and over 200 controls** that focus on the confidentiality of payment card data
- **Merchant and Service Provider levels** are determined by the volume of card transactions processed annually. **Validation and reporting requirements vary**
- A well managed PCI program can help to **significantly reduce the risk** of a breach and payment card data compromise
- **Filing as PCI compliant does not mean an organization is secure!**

PCI Requirement Categories

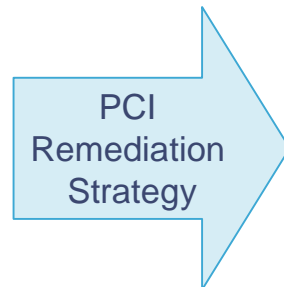
The standard consists of 12 requirements addressing security management, policies, procedures, network architecture and software design for the protection of credit card data. Associated with each requirement are controls used by the Qualified Security Assessor or Internal Audit to determine compliance. (The controls also serve as the basis for the self-assessment questionnaire for merchant levels 2-4.) The six categories and 12 requirements include:

Build and Maintain a Secure Network	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security

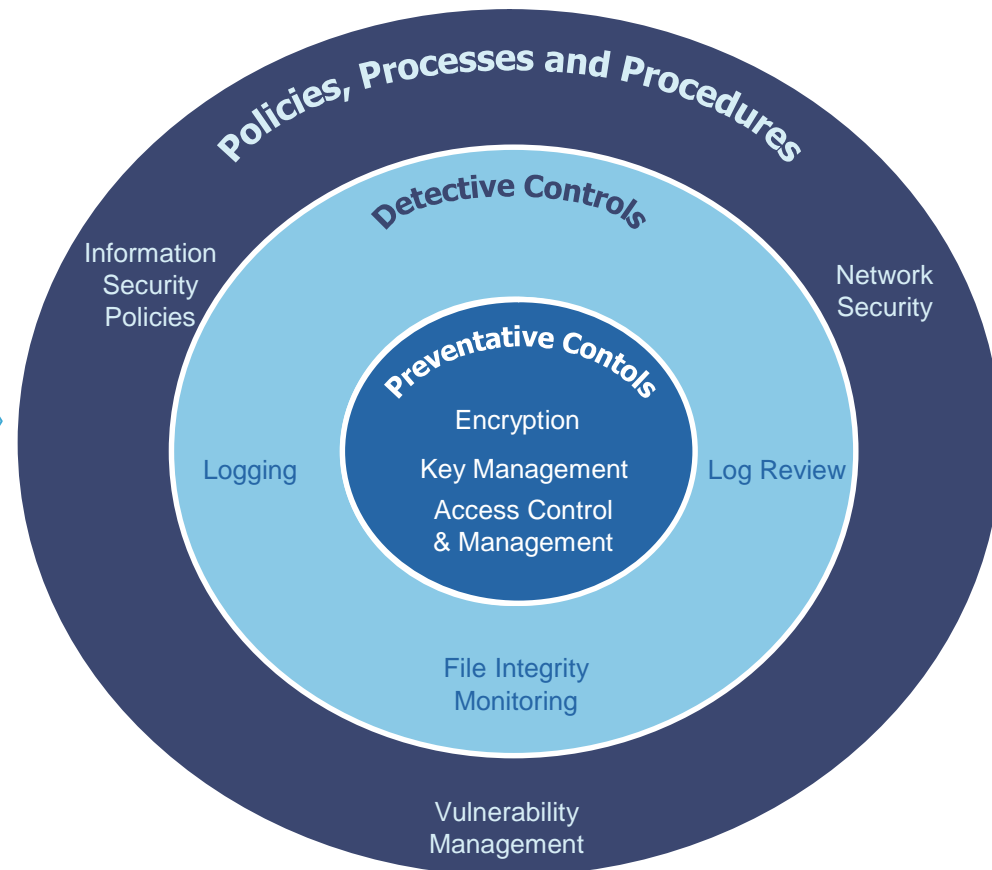
What do PCI Requirements and Controls Focus on?

PCI Data Security Standard Requirements for Compliance

Build & Maintain a Secure Network
Protect Cardholder Data
Maintain a Vulnerability Management Program
Implement Strong Access Control Measures
Maintain an Information Security Policy
Regularly Monitor & Test Networks



Key Focus Areas for PCI Compliance



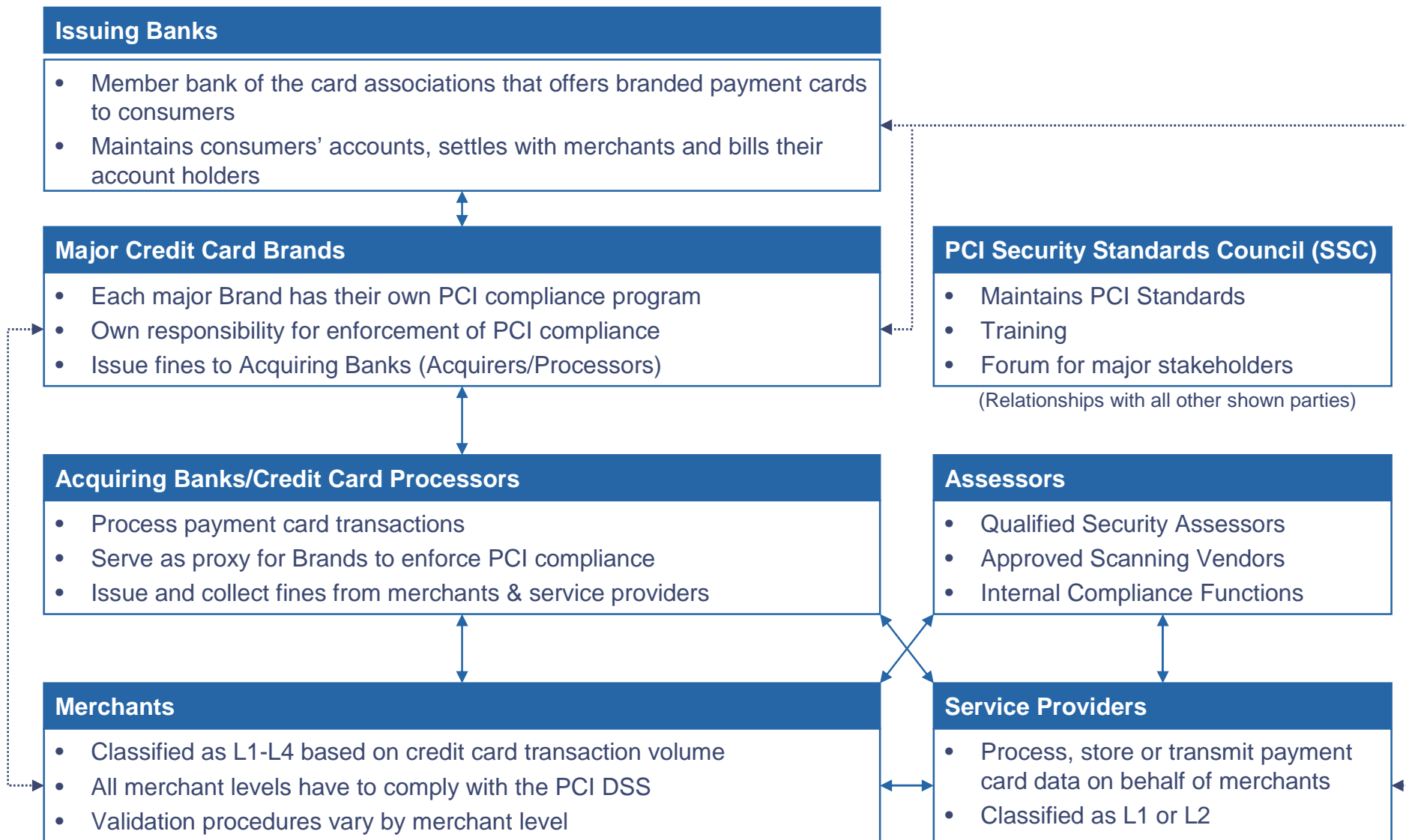
PCI Merchant Levels

Merchant compliance obligations are largely determined by the volume of credit card transactions. A merchant's Acquiring Bank will be able to assist with the validation of transaction volume and corresponding PCI Merchant Level. The following table illustrates Visa's merchant level classification, note that the other leading credit card brands have corresponding classification schemas that may differ from Visa's.

	Level 1	Level 2	Level 3	Level 4
Level Qualifiers:	<ul style="list-style-type: none"> Greater than 6m credit card transactions annually Any company that has been compromised Any business that has been classified as level one by any other credit card company 	<ul style="list-style-type: none"> Between 1-6m credit card transactions per year 	<ul style="list-style-type: none"> Between 20K and 1m credit card, e-commerce, transactions per year 	<ul style="list-style-type: none"> Less than 20K Visa credit card e-commerce, transactions per year Less than 1m traditional Visa credit card transactions MasterCard: merchants with <20K transactions AMEX: merchants with <50K is a Level 3 (lowest level)
PCI DSS Requirements:	<ul style="list-style-type: none"> Annual on-site, data security assessment Quarterly network scans Annual external/internal penetration tests 	<ul style="list-style-type: none"> Annual on-site, data security assessment Quarterly network scans Annual external/internal penetration tests 	<ul style="list-style-type: none"> Annual PCI self-assessment questionnaire Quarterly network scans Annual external/internal penetration tests 	<ul style="list-style-type: none"> Annual PCI self-assessment questionnaire Quarterly network scans Annual external/internal penetration tests
To Be Validated By:	<ul style="list-style-type: none"> Qualified Security Assessor or Internal Audit if signed by Officer* Approved Scanning Vendor (ASV) Any third party vendor 	<ul style="list-style-type: none"> Merchant* ASV 	<ul style="list-style-type: none"> Merchant ASV 	<ul style="list-style-type: none"> Merchant ASV

* By 12/31/2010, Level 1 and 2 merchants will be required to use a QSA to validate compliance

Key PCI Stakeholders and Their Relationships



Note: Arrows represent primary PCI compliance driven relationships; other relationships may exist. An "Open Loop" system is depicted, other payment process configurations and associated relationships exist.

What are Leading Merchants doing to Become PCI Compliant?

Merchants leading in becoming PCI compliant are using the following practices:

- Pursue a balance between a risk and compliance-based approach
- Establish a cross-departmental, enterprise-wide team of key stake holders
- Develop data flow diagrams for the entire payment environment
- Identify and leverage synergy between PCI and other compliance efforts
- Rationalize payment processes and consolidate payment data and systems
- Continuously monitor efforts and identify areas where incremental improvements can be made to further strengthen payment card protection
- Consider “emerging technologies” to reduce the cost and management effort of maintaining compliance

Recent developments in the PCI space

Development #1: Increased focus on all merchant and service provider levels

- Increased focus on smaller merchants
- Changes to the MasterCard's SDP program

Development #2: Emerging payment security solutions are getting a lot of attention

- Stakeholders are looking at ways to reduce the cost and impact of PCI compliance
- Global market research into emerging technologies conducted by PwC

Development #3: Key Dates and Initiatives from the Security Standards Council

- PA-DSS deadlines
- PCI SSC quality assurance program
- PCI feedback program
- New wireless guidance
- Global compliance validation and reporting deadlines for larger merchants

Development #4: Government Involvement

- Nevada State Law – SB 227
- Potential government involvement in the protection of cardholder data

Key PCI Compliance Dates

Date	Description
March 31, 2007	Assertion by merchants that no “prohibited” payment card data is stored by merchants of all levels.
September 30, 2007 (L1) December 31, 2007 (L2)	Full compliance with the PCI standard.
September 30, 2009	Global Prohibited Data Storage Deadline for Level 1 and 2 Merchants (Visa).
October 1, 2009	VisaNet Processors (VNP) and agents must decertify all vulnerable payment applications (Visa).
June 30, 2010	Use of WEP in current wireless implementations prohibited (PCI DSS).
July 1, 2010	TDES Mandate ; all POS PEDs must be encrypting PINs using TDES end-to-end (Visa and MasterCard).
July 1, 2010	Acquirers must ensure their merchants, VNPs and agents use only PA-DSS compliant applications (Visa).
September 30, 2010	Global PCI DSS Compliance Validation Deadline for Level 1 Merchants (Visa) (excludes Visa Europe).
December 31, 2010	All Level 1 and Level 2 merchants must validate compliance and complete an annual onsite assessment conducted by a PCI SSC certified Qualified Security Assessor (MasterCard).

PCI trends

We are observing the following PCI trends:

- Frustration among certain companies about the **quality and inconsistency** of the QSA-mandated PCI compliance validation program
- Merchants and Service Providers claiming that they are spending a **disproportionate amount of resources** on securing payment data
- An increasing number of our clients are asking about **alternative solutions** to lessen their PCI compliance burden
- Our larger clients tend to be more focused on **brand and reputational risk** associated with a potential PCI data breach and are prepared to make additional investments during remediation
- On average, smaller Merchants (L2/L3) demonstrate **significant inconsistencies** in their self-assessment and PCI compliance validation activities; often resulting in residual risk
- As PCI compliance programs reach year 2 and 3 post compliance maturation companies are increasingly showing interest in the **integration of PCI with other enterprise compliance efforts** to improve sustainability and to reduce cost and risk
- We see a noticeable **uptick in demand** for PCI guidance and services in non-US/Canada markets – PCI is going global

Questions