PAYMENT CARD INDUSTRY (PCI) ANNUAL TRAINING

DECEMBER 10, 2009

WESTERN ILLINOIS UNIVERSITY
OFFICE OF THE CTSO & BUSINESS SERVICES

Coalfire
IT Governance and Compliance

Hanson INFORMATION SYSTEMS

The Illinois Funds e-pay Electronic Payment Services Program

ILLINOIS AUDITOR GENERAL

ILLINOIS

AGENDA

- PCI – Players and Roles
- Merchant Requirements
- Keys To Successful PCI Compliance
- Minimize and Conquer
  - Best approach for reducing merchant PCI scope
- Future of the PCI DSS

WHO'S DOING WHAT?

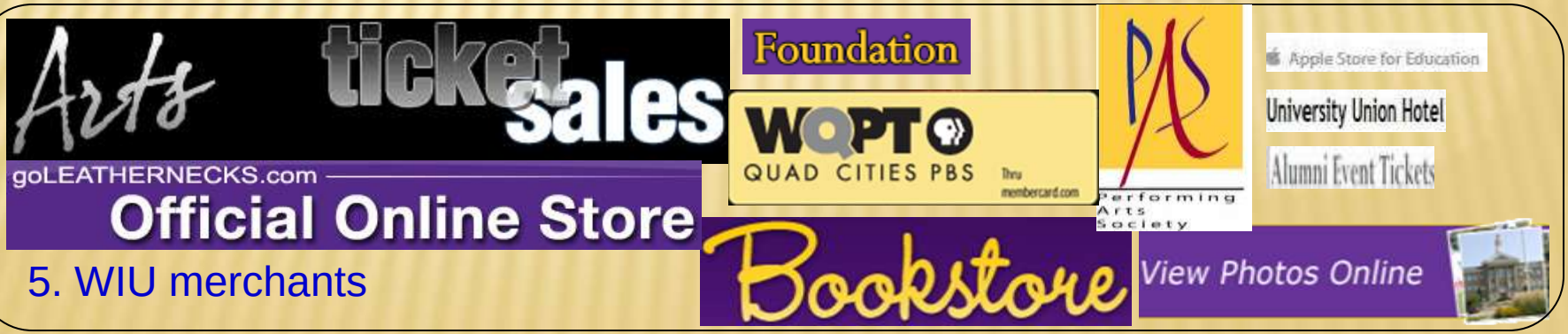
1. Develops Standards

2. Establishes compliance requirements

3. Enforces requirements on merchants

4. Processes Credit Cards for merchants

5. WIU merchants



RESPONSIBILITY FOR COMPLIANCE

PCI Security Standards Council

Part 3. PCI DSS Validation

Based on the results noted in the SAQ D dated *(completion date)*, *(Merchant Company Name)* asserts the following compliance status (check one):

☐ **Compliant:** All sections of the PCI SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; **and** a passing scan has been completed by a PCI SSC Approved Scan Vendor, thereby *(Merchant Company Name)* has demonstrated full compliance with the PCI DSS.

☐ **Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered "yes," resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scan Vendor, thereby *(Merchant Company Name)* has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

Merchant confirms:

☐	PCI DSS Self-Assessment Questionnaire D, Version *(version of SAQ)*, was completed according to the instructions therein.
☐	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☐	I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.
☐	No evidence of magnetic stripe (i.e., track) data[2], CAV2, CVC2, CID, or CVV2 data[3], or PIN data[4] storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. Merchant Acknowledgement

Signature of Merchant Executive Officer ↑	*Date* ↑
Merchant Executive Officer Name ↑	*Title* ↑
Merchant Company Represented ↑	

Scope of Compliance with PCI DSS

The PCI DSS security requirements apply to all system components. — System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications.

MERCHANT LEVELS
DEFINED BY CARD BRAND

Level	American Express	MasterCard	Visa
1	Merchants processing over **2.5 million** AMEX card transactions annually or any merchant that AMEX otherwise deems a Level1.	Merchants processing over **6 million** MasterCard transactions (all channels) annually or compromised merchants.	Merchants processing over **6 million** Visa Transactions annually, identified by another payment card brand as **level 1**, or merchants compromised last year.
2	Merchants processing **50,000 to 2.5 million** AMEX transactions annually, or any merchant that AMEX otherwise deems a Level 2.	Merchants processing **1 million to 6 million** MasterCard transactions annually or any merchant considered Level 2 by another card brand.	Merchants processing **1 million to 6 million** Visa transactions annually.
3	Merchants processing less than **50,000** AMEX transactions annually.	Merchants processing over **20,000 MasterCard e-commerce** transactions annually.	Merchants processing **20,000 to 1 million Visa e-commerce** transactions annually.
4	N/A	All other MasterCard merchants.	Merchants processing less than **20,000 Visa e-commerce** transactions annually, and all other merchants processing up to **1 million** Visa transactions annually.

MERCHANT VALIDATION REQUIREMENTS ENFORCED BY BANKS

Level	American Express	MasterCard	Visa
1	•Onsite Review by a QSA. •Quarterly Network Scan by ASV.	•Onsite Review by a QSA. •Quarterly Network Scan by ASV.	•Onsite Review by a QSA. •Quarterly Network Scan by ASV.
2	•Quarterly Network Scan by ASV.	•Onsite Review by a QSA. •Quarterly Network Scan by ASV.	•Annual Self-Assessment Questionnaire •Quarterly Network Scan by ASV.
3	•Quarterly Network Scan by ASV.	•Annual Self-Assessment Questionnaire •Quarterly Network Scan by ASV.	•Annual Self-Assessment Questionnaire •Quarterly Network Scan by ASV.
4	N/A	•Annual Self-Assessment Questionnaire •Quarterly Network Scan by ASV.	•Annual Self-Assessment Questionnaire •Quarterly Network Scan by ASV.

- ✓What you **must do**, and how you **must validate** are totally separate. (Compliance vs. Validation)
- ✓All merchants **must be** PCI compliant at all times.
- ✓Level 2, 3, and 4 merchants **validate** compliance through the SAQ and quarterly scans (except for MasterCard Level 2 merchants as of June 15, 2009).
- ✓PCI DDS 11.2 requires that all merchants perform external network scanning from an Approved Scan Vendor (ASV).
- ✓QSA stands for Qualified Security Assessor, a designation issued by the PCI SSC to firms/individuals allowing them to conduct audits and submit Reports on Compliance for Level 1 & 2 merchants and Level 1 service providers

MERCHANT VALIDATION REQUIREMENTS THE SAQ

- The PCI DSS consists of 226 control questions spanning 12 requirement categories (the "Digital Dozen"). Technically, all merchants must comply with all 226 control questions.
- In PCI DSS v1.2, the SSC determined that certain merchants could answer a reduced set of questions based on how they accept and handle card data.
- The SSC developed 5 validation types and 4 SAQ's to address this.

SAQ Validation Type	Description	SAQ
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. *This would never apply to face-to-face merchants.*	A
2	Imprint-only merchants with no cardholder data storage	B
3	Stand-alone dial-up terminal merchants, no cardholder data storage	B
4	Merchants with payment application systems connected to the Internet, no cardholder data storage	C
5	All other merchants (not included in descriptions for SAQs A-C above) and **all service providers** defined by a payment brand as eligible to complete an SAQ.	D

SAQS DETAILS

- SAQ A – Web - 13 questions

PCI DSS Requirement	Description of Requirement	Compliance Status (Select One)		Remediation Date and Actions (if Compliance Status is "NO")
		YES	NO	
9	Restrict physical access to cardholder data	☐	☐	
12	Maintain a policy that addresses information security	☐	☐	

- SAQ B – POS/PED – 26 questions

PCI DSS Requirement	Description of Requirement	YES	NO	Remediation Date and Actions (if Compliance Status is "NO")
3	Protect stored cardholder data	☐	☐	
4	Encrypt transmission of cardholder data across open, public networks	☐	☐	
7	Restrict access to cardholder data by business need to know	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
12	Maintain a policy that addresses information security	☐	☐	

- SAQ C – 40 questions from 1-9,11,12
- SAQ D – 226+ questions from all sections

UNDERSTAND YOUR BUSINESS

- ✓Why do you take and keep sensitive data ?
- ✓Where do you store that data?
- ✓What service providers do you work with?
- ✓Are your applications/service providers compliant?
- ✓Who accepts responsibility for compliance?
  - ✓ Up to $25,000 daily fine or loss of merchant privileges
- ✓What contracts do you have?

MINIMIZE & CONQUER

Minimize

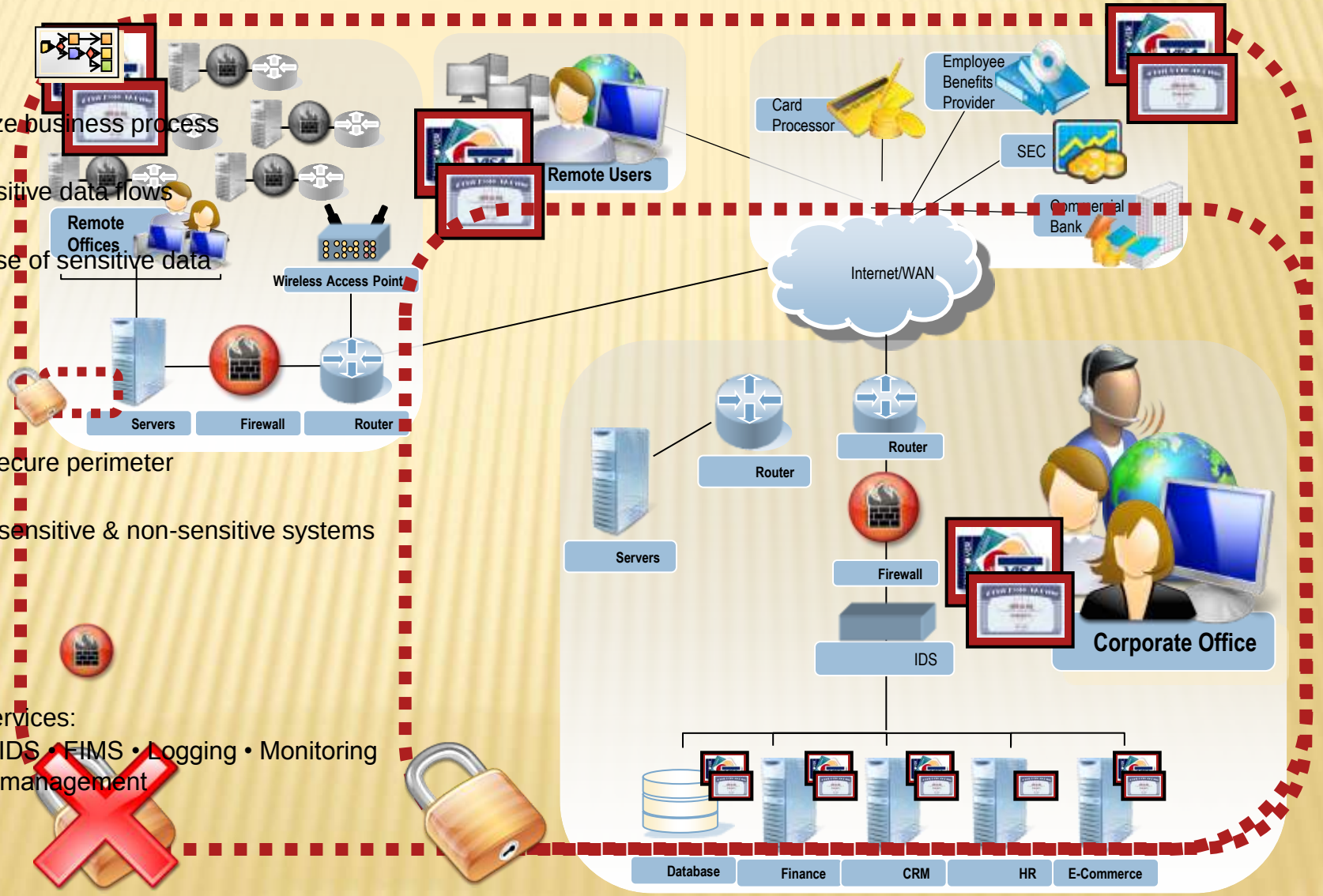
- Characterize business process
- Define sensitive data flows
- Minimize use of sensitive data

Isolate

- Establish secure perimeter
- Segregate sensitive & non-sensitive systems

Protect

- Security Services:
  Firewalls • IDS • FIMS • Logging • Monitoring
  • Vulnerability management



PROTECTING DATA

- Eliminate or Protect Cardholder Data
  - Sensitive Data Scanning
  - Encryption, isolation
- Don’t Use Unprotected Email, FTP, Telnet, Wireless, web 2.0
- Servers
  - Lockdowns - www.wiu.edu/security/securityStandards.php
  - File System Integrity
  - Multi-Factor Authentication
  - Isolation

SECURING WORKSTATIONS

- Personal firewall, IPS, etc.
- Patching
- Network Isolation
  - None or limited Internet Access
  - None or limited Intranet Access
- Full Drive Encryption
- Regular Sensitive Data Scans
- Disable USB, CD/DVD drives, faxing, printing, wireless

VENDOR AGREEMENTS

- PCI DSS 12.8 Security Contract Language in Contracts
  - www.wiu.edu/security/securityStandards.php/InformationSecurityContract.pdf
- Check Your Merchant Agreement or Global Payments Participation Agreement - You as a Merchant Agree to Comply with PCI DSS

PAYMENT APPLICATION DEADLINES

Are your payment applications PCI compliant?

Phase	*Compliance Mandates*	*Effective Date*
I.	Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (VNPs) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications	1/1/08
II.	VNPs and agents must only certify new payment applications to their platforms that are PABP-compliant	7/1/08
III.	Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or use PABP-compliant applications	10/1/08
IV.	VNPs and agents must decertify all vulnerable payment applications	10/1/09
V.	Acquirers must ensure their merchants, VNPs and agents use only PABP-compliant applications	7/1/10

Even if a payment application has been PA-DSS validated, the assessor still needs to verify that the application has been implemented in a PCI DSS compliant manner and environment, and according to the payment application vendor's **PA-DSS Im*plementation Guide***.

All merchants must use ONLY PA-DSS (formerly PABP) certified applications by July 1st, 2010.

PIN ENTRY DEVICE DEADLINES

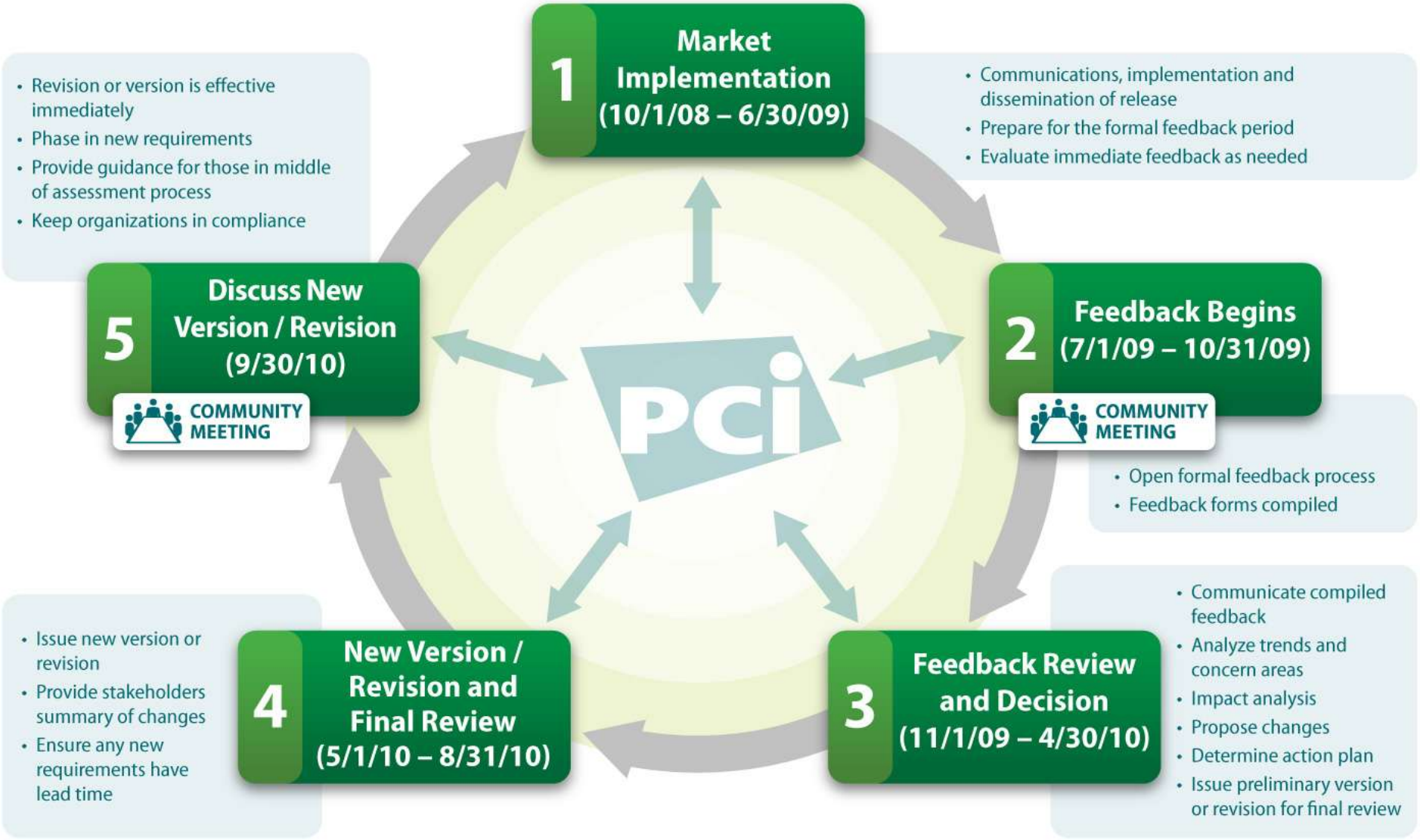
Are your PED Devices PCI compliant?

	Deploy Until	Replace By	Examples
Never Reviewed	N/A	Immediately	VeriFone 380, Nurit 3020
Pre-PCI (VISA PED) compliant	Dec 31 2007	July 2010	VeriFone 3750
PCI PED compliant	N/A	May 2014	VeriFone Vx570

Always purchase your PED device through the business office to ensure your device is PCI PED compliant.

All merchants must use ONLY PCI PED compliant devices by July 1st, 2010.

FUTURE OF THE PCI DSS
PCI DSS UPDATE PROCESS



WHAT'S NEW IN V 1.3 OF THE DSS?

Too early to tell but here are some prospects:

- Risk Assessment
- Wireless
- Encryption
  - Visa published Best Practice document "Data Field Encryption Version 1.0" in October 5, 2009
- Virtualization

MERCHANT VALIDATION REQUIREMENTS RESOURCES

- **The Prioritized Approach** - the PCI SSC has published a "Prioritized Approach" which offers guidance on how to focus PCI DSS control implementation efforts to expedite the security of cardholder data.
  - The Prioritized Approach helps merchants identify how to reduce risk to card holder data as early on as possible. The tool groups the requirements of PCI DSS 1.2 into six key milestones. Get it at:
    https://www.pcisecuritystandards.org/education/prioritized.shtml
- **PCI DSS** - https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- **SAQ's** – https://www.pcisecuritystandards.org/saq/index.shtml
- **Service Providers** - use a PCI certified service provider, get the list at:
  http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf
- **Payment Applications** - Use a PA DSS certified payment application, get the lists at:
  http://usa.visa.com/download/merchants/validated_payment_applications.pdf
  https://www.pcisecuritystandards.org/security_standards/vpa/

THANK YOU – Q & A

Michael Rodriguez – PCI Coordination
(309) 298-4500
ma-rodriguez@wiu.edu

Cheryl Webster – Business Services
(309) 298-1811
CL-Webster@wiu.edu

"80% of data loss resulting from level 4 merchants"
– Illinois State Treasurer's Office