PCI DSS 3.0 Overview

OSU Business Affairs
Business Affairs PIT Crew - Project, Improvement, & Technology
Robin Whitlock

01/16/2015
Purpose of Today’s Presentation

- To provide an overview of PCI 3.0 based on our current understanding, so you can review your security processes and update them to the new standard.

- NOTE: We expect clarification of PCI 3.0 requirements to continue throughout 2015. Therefore, information presented at this meeting is subject to change.
Today’s Presentation

- Purpose of Today’s Presentation
- What is PCI DSS 3.0?
- Who Needs to Comply with PCI DSS?
- When Does PCI DSS 3.0 Start?
- Compliance Life Cycle
- What is Cardholder Data?
- What’s New: PCI DSS 3.0
- Other New 2015 Requirements
- What Do I Need to Do Now?
- SAQ Breakout Sessions
- Resources
- Questions
What is PCI DSS 3.0?

- New version of the PCI Data Security Standard
  - Replaces PCI 2.0
  - New versions every three years
What is PCI DSS 3.0?

- Intended to:
  - Help organizations make payment security part of their business-as-usual activities by introducing more flexibility
  - Increase focus on education, awareness and security as a shared responsibility
Who Needs to Comply with PCI DSS?

- Applies to all entities that store, process or transmit cardholder data (merchants, payment card issuing banks, processors, developers…)
  - That means you!

- Compliance is mandatory
  (eCommerce Policy, Oregon State Treasury, PCI DSS).

- Merchant Managers are responsible for merchant compliance:
  - Attestation
    “I understand that each merchant has fiscal and data security responsibility for proper use of the Merchant ID. I further understand that failure by the merchant to abide by PCI standards could result in fines to the University and/or loss of Merchant ID. To the best of my knowledge, this cover sheet and the information in the attached PCI SAQ (if applicable) accurately represents the operations, procedures, and practices of the Merchant ID's listed above.”
  (Payment Card Industry Data Security Standards Annual Assessment Cover Page).
When Does PCI DSS 3.0 Start?

- Now

- Your December 2015 SAQs submissions will be attestations you are following PCI DSS 3.0 requirements
Compliance Life Cycle

- Pre-Assessment / Gap Analysis should be done now
  - Compare what you are doing now to the new v3.0 requirements in your SAQ
    - Look for what’s broken or where you are not in compliance
    - Fix out of compliance areas
- Implement / RemEDIATE throughout the year
- Complete and submit the PCI-DSS Validation (SAQ) in December
  - 2015 validation will be against the new PCI DSS 3.0 standard
What is Cardholder Data?

- Primary Account Number (PAN)
- Expiration Date
- Cardholder Name

- Chip/Magnetic Strip Data
- CAV2/CVC2/CVV2

What is Cardholder Data?

- Primary Account Number (PAN)
- Expiration Date
- Cardholder Name

- Chip/Magnetic Strip Data
- CAV2/CVC2/CVV2
What’s New: PCI DSS 3.0

- More requirements across the board
- Changes to SAQs
  - Incorporation of new/changed requirements
  - Expected testing added
  - Format updates
- New SAQs: A-EP, B-IP
- Updated eligibility criteria for existing SAQs
More Requirements Across the Board

- Which of the high-level “Digital Dozen” requirements are on each 3.0 SAQ

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>A-EP</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>B-IP</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>C</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>D</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

- SAQs A-EP and B-IP are new 3.0 SAQs
- Requirement 10 is new to SAQ C with 3.0
More Requirements Across the Board

- **PCI DSS Summary of Changes v2.0 to v3.0** is a 12-page document
- Number of changes to requirements:

<table>
<thead>
<tr>
<th>Requirement</th>
<th># of Changes</th>
<th>Requirement</th>
<th># of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>8</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>
More Requirements Across the Board – Some Key Changes

- Requirement 11.3 penetration testing requirements are significantly updated, including
  - Must follow “industry-accepted penetration testing methodology”
  - Verify methods used to segment cardholder data environment from other areas
  - Best practice until June 30, 2015, then a requirement
- New requirement 2.4 requires an inventory be maintained of system components in scope
  - Refers to all hardware and software within the cardholder data environment
  - Include what the components do and why
- Requirements 12.8.5 and 12.9 require specific documentation about which PCI requirements are managed by the vendor and which are managed by the organization

Source: [PCI DSS Version 3.0: The five most important changes for merchants](https://www.pcisecuritystandards.org/assets/documents/670/PCI_DSS_V3_0_White_Paper.pdf)
More Requirements Across the Board – Some Key Changes

- Requirement 5 has some notable changes
  - 5.1.2 states merchants must “identify and evaluate evolving malware threats for systems considered to be not commonly affected by malicious software”
  - 5.3 requires specific authorization from management to disable or alter antivirus operation
- Requirement 9.9 requires that merchants “protect devices that capture payment card data… from tampering and substitution.”

Source: PCI DSS Version 3.0: The five most important changes for merchants
Changes to SAQs
Incorporation of New/Changed Requirements

SAQ Change Summary

<table>
<thead>
<tr>
<th>SAQ Type</th>
<th>v3.0 # of Questions</th>
<th>Change # from v2.1</th>
<th>ASV Scan Required v3.0</th>
<th>Penetration Test Required v3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>14</td>
<td>+1</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>A-EP</td>
<td>139</td>
<td>NEW</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>B</td>
<td>41</td>
<td>+12</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>B-IP</td>
<td>83</td>
<td>NEW</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>C</td>
<td>139</td>
<td>+59</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>D</td>
<td>326</td>
<td>+38</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- Details will be covered in breakout sessions

Expected Testing Added

- New SAQ column “Expected Testing” describes testing activities to be performed during the self-assessment to determine whether a requirement has been met.
- Details will be covered in breakout sessions
  - Sample shown on the following slide “Formal Updates”
Format Updates

**New Landscape orientation**

New column “Expected Testing” describes testing activities to be performed during the self-assessment to determine whether a requirement has been met.

**Sections reorganized.** AOC Parts 3 and 4 now follow the questionnaire.

**2 new columns replace v2.0 single “Special” column**

Additional guidance is provided at the beginning of the SAQ to assist with understanding how to complete it.

---

**Section 2: Self-Assessment Questionnaire A**

*Note: The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the PCI DSS Requirements and Security Assessment Procedures document.*

**Requirement 9:** Restrict physical access to cardholder data

<table>
<thead>
<tr>
<th>PCI DSS Question</th>
<th>Expected Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5 Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? For purposes of Requirement 9, “media” refers to all paper and electronic media containing cardholder data.</td>
<td>• Review policies and procedures for physically securing media  • Interview personnel</td>
</tr>
<tr>
<td>9.6 (a) Is strict control maintained over the internal or external distribution of any kind of media? (b) Do controls include the following:</td>
<td>• Review policies and procedures for distribution of media</td>
</tr>
</tbody>
</table>
New SAQ A-EP Intent

- Developed to differentiate between merchants that have partially outsourced management of their e-commerce transactions, and merchants that have completely outsourced all management of their e-commerce environment (SAQ A merchants).
NEW SAQ: SAQ A vs. SAQ A-EP

- **SAQ A:**
  - The merchant has no direct control of the manner in which cardholder data is captured, processed, transmitted or stored.
  - The entirety of all payment pages delivered to the customer’s browser originates directly from a third-party PCI DSS validated service provider.
    - If any element of a payment page delivered to consumers’ browsers originates from the merchant’s website, SAQ A does not apply.

- **SAQ A-EP:**
  - The merchant website controls how the cardholder data is redirected to the third-party service provider.
SAQ A or SAQ-A-EP?

- If you completed SAQ A for 2014, meet all other SAQ A eligibility requirements, and you have a TouchNet Marketplace uStore or uPay site, TouchNet’s guidance is:
  - Your merchant is still eligible for SAQ A in 2015 under v3.0

- If you completed an SAQ A for 2014 and your payments do not go through TouchNet:
  - You will need to contact your service provider to determine whether SAQ A or SAQ-EP will need to be completed in 2015 and communicate any decision and reasoning to Business Affairs.
Eligibility: SAQ A

- Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions
- All payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service providers
- Merchant has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored
- Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions
  - NO manual entry of cardholder data by OSU is allowed
  - Ex. Cannot take credit card number over phone and enter into TouchNet for customer
- Merchant has confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant,
- Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically
- Additionally, for 3-commerce channels:
  - The entirety of all payment pages delivered to the consumer’s browser originates directly from a third-party PCI DSS validated service provider(s)
Eligibility: NEW SAQ A-EP

- Merchant accepts only e-commerce transactions
- All processing of cardholder data is outsourced to a PCI DSS validated third-party payment processor
- Merchant’s e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor.
- Merchant’s e-commerce website is not connected to any other systems within merchant’s environment (this can be achieved via network segmentation to isolate the website from all other systems)
- If the merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider)
- All elements of payment pages that are delivered to the consumer’s browser originate from either the merchant’s website or a PCI DSS compliant service provider(s)
- Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions
- Merchant has confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant,
- Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically
New SAQ B-IP Intent

- Developed to differentiate between merchants using only standalone payment terminals that connect to their payment processors via an IP-based connection, from merchants who connect to their payment processor using only dial-out connections (which may meet the criteria of SAQ B).
NEW SAQ: SAQ B vs. SAQ B-IP

**SAQ B:**
- Standalone, dial-out terminal
  - Connected via phone line (dial-up or cellular) to the processor
- Cardholder data (CHD) is not transmitted over a network (either internal network or internet)

**SAQ B-IP:**
- Standalone, PTS-approved point-of-interaction (POI) devices (excludes SCRs)
  - Connected via IP to the payment processor
- Only CHD transmission is via IP from the PTS-approved POI devices to the payment processor
SAQ B or SAQ B-IP?

- If you completed SAQ B for 2014, meet all other SAQ B eligibility requirements, and your merchant still uses a standalone, dial-out terminal connected to the processor via phone line (either dial-up or cellular)
- AND
- Cardholder data is not transmitted over a network (does not apply to cellular network)
  - Your merchant is most likely still eligible for SAQ B in 2015 under v3.0.

- If you completed an SAQ B for 2014 but your merchant no longer fits the SAQ B criteria,
  - Please contact Business Affairs for a discussion about SAQ B-IP.
Eligibility: SAQ B

- Merchant uses only an imprint machine to imprint customers’ payment card information and does not transmit cardholder data over either a phone line or the internet, and/or
- Merchant uses only standalone, dial-out terminals (connected via a phone line to your processor); and the standalone, dial-out terminals are not connected to the internet or any other systems within the merchant environment
- Merchant does not transmit cardholder data over a network (either an internal network or the Internet)
- Merchant does not store cardholder data in electronic format and
- If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically
Eligibility: NEW SAQ B-IP

- Merchant uses only standalone, PTS-approved point-of-interaction (POI) devices (excludes SCRs) connected via IP to merchant’s payment processor to take customers’ payment card information
- The standalone IP-connected POI devices are validated to the PTS POI Program as listed on the PCI SCC website (excludes SCRs)
- The standalone IP-connected POI devices are not connected to any other systems within the merchant environment (this can be achieved via network segmentation to isolate POI devices from other systems)
- The only transmission of cardholder data is from the PCI-approved POI devices to the payment processor
- The POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor
- Merchant retains only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically
- Merchant does not store cardholder data in electronic format
Eligibility: SAQ C

- Merchant has a payment application system and an internet connection on the same device and/or same local area network (LAN)
- The payment application system/internet device is not connected to any other system within the merchant environment
- The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single location only
- Merchant does not store cardholder data in electronic format
- If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically
Eligibility: SAQ D

- SAQ-eligible merchants not meeting the criteria for any other SAQ type
- Examples include but not limited to:
  - E-commerce merchants who accept cardholder data on their website
  - Merchants with electronic storage of cardholder data
  - Merchants that don’t store cardholder data electronically but that do not meet the criteria of another SAQ type
  - Merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment
Other New 2015 Requirements
New 2015: QSA Requirement

- Treasury may require universities to engage with a Qualified Security Assessor (like CoalFire) for 2015 PCI
  - No firm details are available yet
  - Requirement is expected to be phased in
    - Most likely begin with SAQ C and D merchants
Starting in 2015, PCI compliance will be included in the annual audit plan by the OSU Office of Audit Services.
- Tentatively scheduled April-June timeframe
- Scope details to be determined
- See Audit process
New 2015: 1st Level 3 Merchant

- OSU first Level 3 merchant in 2015 – OSU Admissions Web
- Rest of OSU merchants are still Level 4

<table>
<thead>
<tr>
<th>Level/Tier</th>
<th>Merchant Criteria</th>
<th>Validation Requirements</th>
</tr>
</thead>
</table>
| 1          | Merchants processing over 6 million Visa transactions annually (all channels) | • Annual Report on Compliance by Qualified Security Assessor (“QSA”)  
• Quarterly network scan by Approved Scan Vendor (“ASV”)  
• Attestation of Compliance Form |
| 2          | Merchants processing 1 million to 6 million Visa transactions annually (all channels) | • Annual Self-Assessment Questionnaire  
• Quarterly network scan by ASV  
• Attestation of Compliance Form |
| 3          | Merchants processing 20,000 to 1 million Visa e-commerce transactions annually | • Annual SAQ  
• Quarterly network scan by ASV  
• Attestation of Compliance Form |
| 4          | Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually | • Annual SAQ  
• Quarterly network scan by ASV if applicable  
• Requirements set by acquirer |
What Do I Need to Do Now?

• Pre-Assessment/Gap Analysis
  • Compare what you are doing now to the new v3.0 requirements in your SAQ
  • Review SAQ eligibility requirements
    • Determine which 3.0 SAQ applies to your merchant
  • Look for what’s broken or where you are not in compliance
  • Fix out of compliance areas
SAQ Breakout Sessions

- SAQ A and A-EP right after this meeting
- To be scheduled in the next few weeks:
  - SAQ B/B-IP
  - SAQ C
  - SAQ D
Resources

- Annual PCI Compliance for OSU Credit Card Merchants (instructions & forms)
- Payment Card Industry Data Security Standards (PCI DSS)
- OSU FIS Manual
- Oregon State Treasury Policy Guideline for Electronic Commerce
- Oregon Accounting Manual - Credit Card Acceptance for Payment
- Oregon State Treasury Cash Management Policy

Please note in some Powerpoint versions, the presentation must be in Slide Show mode for the links to work.
Thank You

Business Affairs Contacts

- Robin Whitlock
  - Robin.Whitlock@OregonState.edu, 541-737-0622
Backup Slides
1. These data elements must be protected if stored in conjunction with the PAN.
2. Sensitive authentication data must not be stored after authorization (even if encrypted).
3. Magnetic stripe or chip.
PCI DSS Goals & Requirements

Build and Maintain a Secure Network (2)
1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other parameters

Protect Cardholder Data (2)
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
PCI DSS Goals & Requirements

Maintain a Vulnerability Management Program (2)
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures (3)
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
PCI DSS Goals & Requirements

**Regularly Monitor and Test Networks (2)**
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

**Maintain an Information Security Policy (1)**
12. Maintain a policy that addresses information security