

What's New in PCI DSS v3.0?



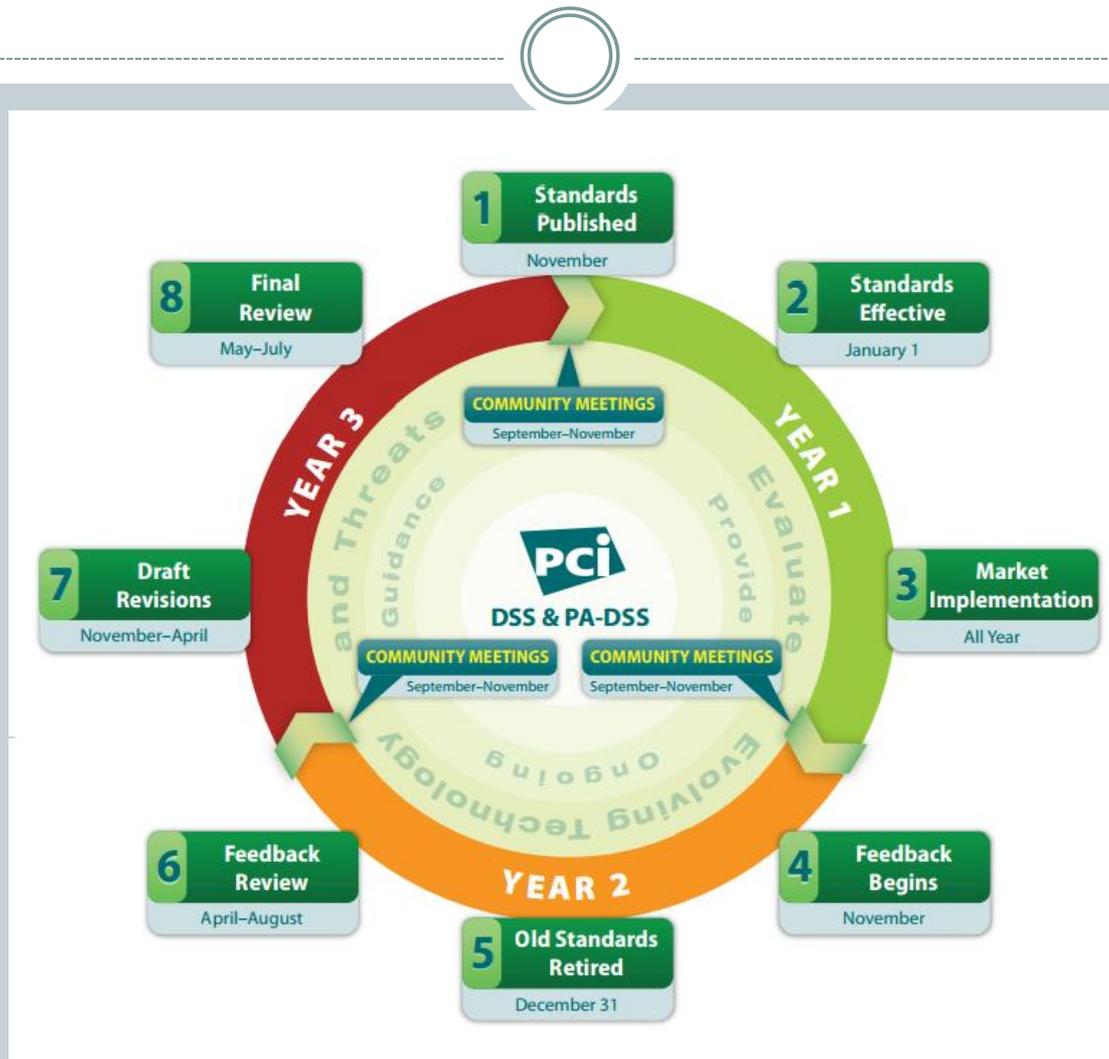
SHANA BUMPAS, MSIA, CISSP, CISA, PCIP
VIRGINIA DEPARTMENT OF TAXATION
APRIL 3, 2015

History of PCI



- Card brands had individual programs since late 90s
- PCI DSS version 1.0 introduced in December 2004
- Standard updated to version 1.1 in September 2006
 - PCI Security Standards Council formed
- Version 2.0 released in October 2010
- Version 3.0 released in October 2013

PCI DSS Lifecycle



The Gist



- PCI DSS v3.0 effective January 1, 2014
- Requirements more prescriptive, provide clarification, and are evolving
- New Self Assessment Questionnaires (SAQ) available

New SAQs



A-EP*	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. <i>Applicable only to e-commerce channels.</i>
B-IP*	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>

Existing SAQs: A, B, C, C-VT, D, and P2PE-HW

Changes



- Network diagram must show card data flow (Req 1)
- Inventory of components in scope (Req 2)
- Evaluate evolving threats on systems not commonly infected with malware (Req 3)
- Antivirus actively running and cannot be disabled or altered (Req 5)
- Code required to protect against broken authentication and session* (Req 6)

Changes cont.



- Flexibility with alternative password requirements (Req 8)
- Service Providers (SP) to use unique authentication* (Req 8)
- Other authentication mechanisms must be linked to an individual account (Req 8)
- Control physical access to sensitive areas for onsite personnel (Req 9)
- Physical protection of payment capturing devices* (Req 9)

Changes cont.



- Use and changes to identification and authentication mechanisms logged (Req 10)
- Include stopping and pausing of audit logs (Req 10)
- Maintain inventory of authorized wireless APs along with documented business justification (Req 11)
- Implement incident response procedure for rogue APs when detected (Req 11)
- Implement methodology for pen testing* (Req 11)

Changes cont.



- Implement process to respond to any file change-detection alerts (Req 11)
- Risk assessment should be at least annually and after significant changes (Req 12)
- Identify requirements managed by SP and entity (Req 12)
- SPs to provide written agreement/acknowledgement to customers (Req 12)
- Document security polices and operational procedures (All)

Liability Shift



- EMV Chip and Pin becoming required
- Acquirers and processors are EMV ready April 2013
- Shift liability policy for POS effective October 2015
- Fuel dispensers by October 2017
- ATMs EMV ready October 2016 for MasterCard and 2017 for VISA

References



- American Express Data Security, https://www260.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=home&ln=en&frm=US
- JCB Data Security Program, <http://partner.jcbcard.com/security/jcbprogram/index.html>
- MasterCard Site Data Protection and PCI, http://www.mastercard.com/us/company/en/whatwedo/site_data_protection.html
- PCI Security Standards Council, <https://www.pcisecuritystandards.org>
- PCI Security Standards Council LLC. 2014. Lifecycle for Changes to PCI DSS and PA-DSS. Retrieved from [https://www.pcisecuritystandards.org/pdfs/Lifecycle for Changes to PCI DSS and PA-DSS.pdf](https://www.pcisecuritystandards.org/pdfs/Lifecycle_for_Changes_to_PCI_DSS_and_PA-DSS.pdf)
- PCI Security Standards Council LLC. 2014. Understanding the SAQs for PCI DSS v3.0. Retrieved from [https://www.pcisecuritystandards.org/documents/Understanding SAQs PCI DSS v3.pdf](https://www.pcisecuritystandards.org/documents/Understanding_SAQs_PCI_DSS_v3.pdf)
- VISA Cardholder Information Security Program, http://usa.visa.com/merchants/risk_management/cisp.html?ep=v_sym_cisp