MASC Municipal Association of South Carolina

PCI SSC Community Meeting Update: PCI DSS v3.0 Planned Changes

Ray Hillen | Director of Security Practice

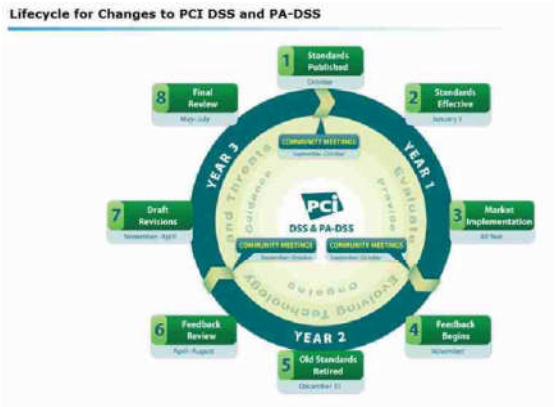
March 2013

SecureEnterprise COMPUTING

The PCI DSS Lifecycle

1

- The PCI DSS follows a three-year lifecycle
- PCI DSS 3.0 will be released in November 2013
- Optional (but recommended) in 2014; Required in 2015



SecureEnterprise COMPUTING

Key Themes

2

- Education and awareness
- Flexibility and consistency
- Security as a shared responsibility
- Emerging threats

SecureEnterprise COMPUTING

Best Practices for Implementing PCI DSS Into Business As Usual (BAU) Processes

3

- Continuous compliance with due diligence needed
- PCI DSS is not a “once-a-year” activity
- Don’t forget about the people and processes

SecureEnterprise COMPUTING

Administrative Improvements

4

- Enhanced sampling examples and testing procedures for each requirement
- Enhanced reporting guidance
  - *Navigation Guide* integrated into PCI DSS v3.0
- New templates (ROC/SAQ)
  - ROC reporting instructions built into the ROC template
  - Easier to complete, more concise
  - Visual queues for when diagrams are needed
- Policy and procedure requirements moved from Section 12 to each individual section

SecureEnterprise COMPUTING

Administrative Improvements (Cont'd)

5

- Added flexibility to meet requirements:
  - Passwords
  - Web application firewalls
  - File integrity monitoring (FIM)
  - Inventory/labeling options
- NEW requirements listed in this presentation are either a requirement as of January 1, 2015 or a best practice until June 30, 2015, after which they become mandatory requirements (see list).
- Note: Cannot mix and match v2.0 and v3.0 – must use one or the other next year

SecureEnterprise COMPUTING

Scoping Guidance

6

- Improper scoping leads to increased risk
  - Look at people and process
- Focus on security, rather than compliance
- Not a one-time-a-year activity
- Confirm effectiveness of PCI scope (pen test)
- Goal: reduce complexity and create more efficient security
- Risk assessments as scoping aid

SecureEnterprise COMPUTING

Clarifications for Segmentation

7

- Isolation is clarified
- Controlled access means a connection exists, therefore those systems are in scope (AD, AV, DNS, time servers, etc.)
- Improved language to verify effectiveness

SecureEnterprise COMPUTING

Changes – Requirement 1
"Build and Maintain a Secure Network and Systems"

8

- Clarifications:
  - Configuration standards must be documented and implemented (1.1.x)
  - Network diagram & CHD flows (1.1.2-1.1.3)
  - Insecure services, protocols, ports (1.1.6)
  - Securing router configuration files (1.2.2)
  - Wireless access control to CDE (1.2.3)
  - Anti-spoofing (1.3.4)
  - Access to CDE from untrusted networks (1.3.7)
  - Requirement and testing procedures (1.4)

SecureEnterprise COMPUTING

Changes – Requirement 2
"No Vendor Defaults"

9

- Clarifications:
  - Change <u>all</u> default passwords; remove unnecessary default accounts (2.1)
  - Change all wireless default passwords at installation (2.1.1)
  - Include the above in Configuration Standards (2.2)
  - Enable only necessary/secure services, protocols, and ports (2.2.2-2.2.3)

SecureEnterprise COMPUTING

Changes – Requirement 2
"No Vendor Defaults"

10

- **NEW** Requirement:
  - Maintain an inventory of all systems and components that are in scope for PCI DSS

REQUIRED BY JAN 1, 2015

SecureEnterprise COMPUTING

Changes – Requirement 3
"Protect Stored Cardholder Data (CHD)"

11

- Clarifications:
  - Data Retention and Disposal (3.1.x)
  - Sensitive Authentication Data (SAD) proper destruction after authorization (3.2)
  - Primary Account Number (PAN) masking (3.3)
  - Separation of OS and Disk-level encryption authentication mechanisms (3.4.1)
  - Key Management procedures (3.5)
  - Provided flexibility with more options for secure storage of cryptographic keys (3.5.2-3.5.3)
  - Testing implementation of crypto key management (3.6.x)
  - Crypto key "split-knowledge" and "key control" (3.6.6)

SecureEnterprise COMPUTING

Changes – Requirement 4
"Encrypt transmission of CHD across untrusted networks"

12

- Clarifications:
  - Expanded examples of open public networks (4.1)

SecureEnterprise COMPUTING

Changes – Requirement 5
"Maintain a Vulnerability Management Program"

13

- Clarifications:
  - Ensure all AV mechanisms are maintained properly (5.2)
- **NEW** Requirements:
  - REQUIRED BY JAN 1, 2015 Systems not commonly affected by malware must be evaluated (5.1.2)
  - REQUIRED BY JAN 1, 2015 Ensure AV is running and cannot be disabled/altered (5.3)

SecureEnterprise COMPUTING

Changes – Requirement 6
"Develop & Maintain Secure Systems and Applications"

14

- Clarifications:
  - Identifying, risk ranking, and patching critical vulnerabilities (6.1-6.2)
  - Written software development procedures (6.3)
  - Development and Test environments (6.3.1)
  - Enhanced testing procedures that include document reviews (6.4)
  - Enforce separation of production and development environments with access controls (6.4.1)
  - Updated list of current and emerging coding vulnerabilities and secure coding guidelines (6.5.x)
  - Options beyond Web Application Firewall provided (6.6)

SecureEnterprise COMPUTING

Changes – Requirement 6
"Develop & Maintain Secure Systems and Applications"

15

- **NEW** Requirements:
  - REQUIRED BY JUL 1, 2015 Handling of PAN and SAD in memory (6.5.6)
  - REQUIRED BY JUL 1, 2015 Coding practices to protect against broken authentication and session management (6.5.11)

SecureEnterprise COMPUTING

Changes – Requirement 7
"Restrict Access to CHD by Business Need-to-Know"

16

- Clarifications:
  - Revised testing procedures (7.1)
  - Definition of access needs for each role (7.1.1)
  - Restrict Privileged User IDs to least necessary (7.1.2)
  - Assign access based upon role/classification (7.1.3)

SecureEnterprise COMPUTING

Changes – Requirement 8
"Identify and Authenticate Access to System Components"

17

- Clarifications:
  - User identification (8.1)
  - Remote vendor access (8.1.5)
  - User authentication (8.2)
  - Changed passwords to passphrases/authentication credentials
  - Requirements apply to 3rd Party Vendors
  - Strong cryptography for authentication credentials (8.2.1)
  - Authenticate users prior to modifying credentials (8.2.2)

SecureEnterprise COMPUTING

Changes – Requirement 8
"Identify and Authenticate Access to System Components"

18

- Clarifications:
  - Requirements 8.1.1, 8.1.6-8.1.8, 8.2, 8.5, and 8.2.3-8.2.5 are not intended to apply to user accounts within a point-of-sale (POS) application that only has access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).
  - Two-factor authentication applies to users, administrators, and all third-parties (8.3)
  - How to protect authentication credentials (8.4)

SecureEnterprise COMPUTING

Changes – Requirement 8
"Identify and Authenticate Access to System Components"

19

- **NEW** Requirements:
  - REQUIRED BY JAN 1, 2015 — Options provided beyond passwords (tokens, smart cards, and certificates) for equivalent variations (8.2.3)
  - REQUIRED BY JUL 1, 2015 — Service Providers with access to customer environments must use a unique authentication credential (e.g., password) for each customer environment (8.5.1)
  - REQUIRED BY JAN 1, 2015 — Physical security tokens must be capable of being linked to an individual account (8.6)

SecureEnterprise COMPUTING

Changes – Requirement 9
"Restrict Physical Access to Cardholder Data"

20

- Clarifications:
  - Protection of network jacks (9.1.2)
  - Differentiation between on-site personnel and visitors – options made available (9.2.x)
  - Visitor audit trails (9.4.x)

SecureEnterprise COMPUTING

Changes – Requirement 9
"Restrict Physical Access to Cardholder Data"

21

- **NEW** Requirements:
  - REQUIRED BY JAN 1, 2015 Control physical access to sensitive areas for on-site personnel (9.3)
  - REQUIRED BY JUL 1, 2015 Protect POS terminals and devices from tampering or substitution (9.9)

SecureEnterprise COMPUTING

Changes – Requirement 10
"Track and Monitor All Access to Network Resources and Cardholder Data"

22

- Clarifications:
  - Audit trails linked to individuals (10.1)
  - Clarified the intent and scope of daily log reviews (10.6)

SecureEnterprise COMPUTING

Changes – Requirement 10
"Track and Monitor All Access to Network Resources and Cardholder Data"

23

- **NEW** Requirements:
  - REQUIRED BY JAN 1, 2015 All changes to identification and authentication mechanisms and all changes to root or administrator access must be logged (10.2.5)
  - REQUIRED BY JAN 1, 2015 Pausing, stopping, and restarting of audit logs must be logged (10.2.6)

SecureEnterprise COMPUTING

Changes – Requirement 11
"Regularly Test Security Systems and Processes"

24

- Clarifications:
  - Added guidance regarding multiple scan reports (11.2)
  - Quarterly internal vulnerability scans must be repeated until a passing scan results (11.2.2)
  - Internal and External scans must be performed after significant changes (11.2.3)
  - Correct all vulnerabilities detected during a Penetration Test (11.3.3)
  - Methods expanded for detecting changes to files (11.5)

SecureEnterprise COMPUTING

Changes – Requirement 11
"Regularly Test Security Systems and Processes"

25

- **NEW** Requirements:
  - REQUIRED BY JAN 1, 2015 Have an inventory and business justification for wireless access points (11.1.x)
  - REQUIRED BY JUL 1, 2015 Implement a methodology for penetration testing, and perform penetration tests to verify that the segmentation methods are operational and effective (11.3)
  - REQUIRED BY JAN 1, 2015 Develop process to respond to change detection alerts (11.5.1)

SecureEnterprise COMPUTING

Changes – Requirement 12
"Maintain a Policy that Addresses Security for all Personnel"

26

- Clarifications:
  - Policy and procedure requirements moved from section 12 to each individual section
  - Added options regarding identification (labeling) of devices (12.3.4)
  - Testing of remote access timeouts (12.3.8)
  - Management of Service Providers (12.8)
  - Further defined the components of Incident Response plan (12.10.x)

SecureEnterprise COMPUTING

Changes – Requirement 12
"Maintain a Policy that Addresses Security for all Personnel"

27

- **NEW** Requirements:
  - REQUIRED BY JAN 1, 2015 Risk Assessment should be performed at least annually and after significant changes (12.2)
  - REQUIRED BY JAN 1, 2015 Maintain separation of duties for security responsibilities (12.4.1)
  - REQUIRED BY JAN 1, 2015 Clarified essential components of Service Provider agreements (12.8.2)
  - REQUIRED BY JUL 1, 2015 Maintain information about which PCI DSS requirements are managed by service providers and which are managed by the entity (12.8.5). Service providers to acknowledge responsibility for maintaining applicable PCI DSS requirements. (12.9)

SecureEnterprise COMPUTING

Next Steps – How to Prepare

28

- Review the clarifications to ensure compliance
- Verify effective segmentation of CDE
- Look at day-to-day PCI compliance efforts
  - Are Configuration Standards current?
  - Are diagrams current?
  - Are security procedures current and being followed?
- Review asset inventory process (2.x); ensure it includes all CDE systems and any wireless access points (11.2)
- Consider AV options for increased coverage (5.1.2)
- Ensure AV is locked down (5.3)

SecureEnterprise COMPUTING

Next Steps – How to Prepare

29

- Ensure the ***Risk Ranking Procedure*** is documented and followed (6.2)
- Review *PA DSS Implementation Guides*
  - How is PAN/SAD stored in memory managed? (6.5.6)
- Review session management coding practices (6.5.11)
- Review how service providers are managed
  - Access management - no shared IDs/accounts (8.5.1)
  - Fully PCI compliant (12.8)
  - Review contracts, clearly define responsibilities (12.8.2)
  - Ensure the SP acknowledges responsibilities (12.9)

SecureEnterprise COMPUTING

Next Steps – How to Prepare

30

- Review security tokens and ensure each is linked to a unique individual (8.6)
- Review on-site personnel access controls to sensitive areas (9.3)
- Consider methods to prevent tampering with POS equipment (9.9)
- Review log security settings (admins, stop/start, etc.) (10.2.5-6)
- If wireless is used, document the business justification (11.1)
- Ensure penetration test methodology is documented (11.3)
- Ensure vulnerabilities detected are corrected and then retest to ensure compliance for Internal scans (11.2.2) and penetration tests (11.3.3)

SecureEnterprise COMPUTING

Next Steps – How to Prepare

31

- Ensure security alerts (FIM/IDS/etc.) are integrated into incident response process (11.5.1)
- Verify that remote access timeouts are working properly (12.3.8)
- Verify that risk assessments are performed both annually and after significant changes to CDE are made (12.2)
- Ensure separation of duties exists for information security (12.4.1)
- Review and update the incident response plan (12.10)

SecureEnterprise COMPUTING

Questions?

Contact Us

Ray Hillen, *Director, Security Practice*
rhillen@secure-enterprise.com

Justin Smith, *Account Manager*
jsmith@secure-enterprise.com

Laurie Leigh, *Director of Sales*
lleigh@secure-enterprise.com

Mike Milligan, *Account Manager*
mgm@secure-enterprise.com

SECURE ENTERPRISE COMPUTING,
AN AGIO COMPANY

909 Aviation Parkway, Suite 600
Morrisville, NC 27560
phone 919.380.7979
fax 919.380.9055
web www.secure-enterprise.com

SecureEnterprise
COMPUTING