CHANGES TO PCI DSS FROM V 1.2.1 TO V 2.0

Panaiyur S Gopalakrishnan
PCI Qualified Security Assessor
M.Kuppuswamy PSG & Co
psg@mkpsg.com
+919884133386

OWASP
January 8, 2011

The OWASP Foundation
http://www.owasp.org

Payment Card Industry Security Standards Council

- The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) Requirements.

- The Council's five founding global payment brands -- American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

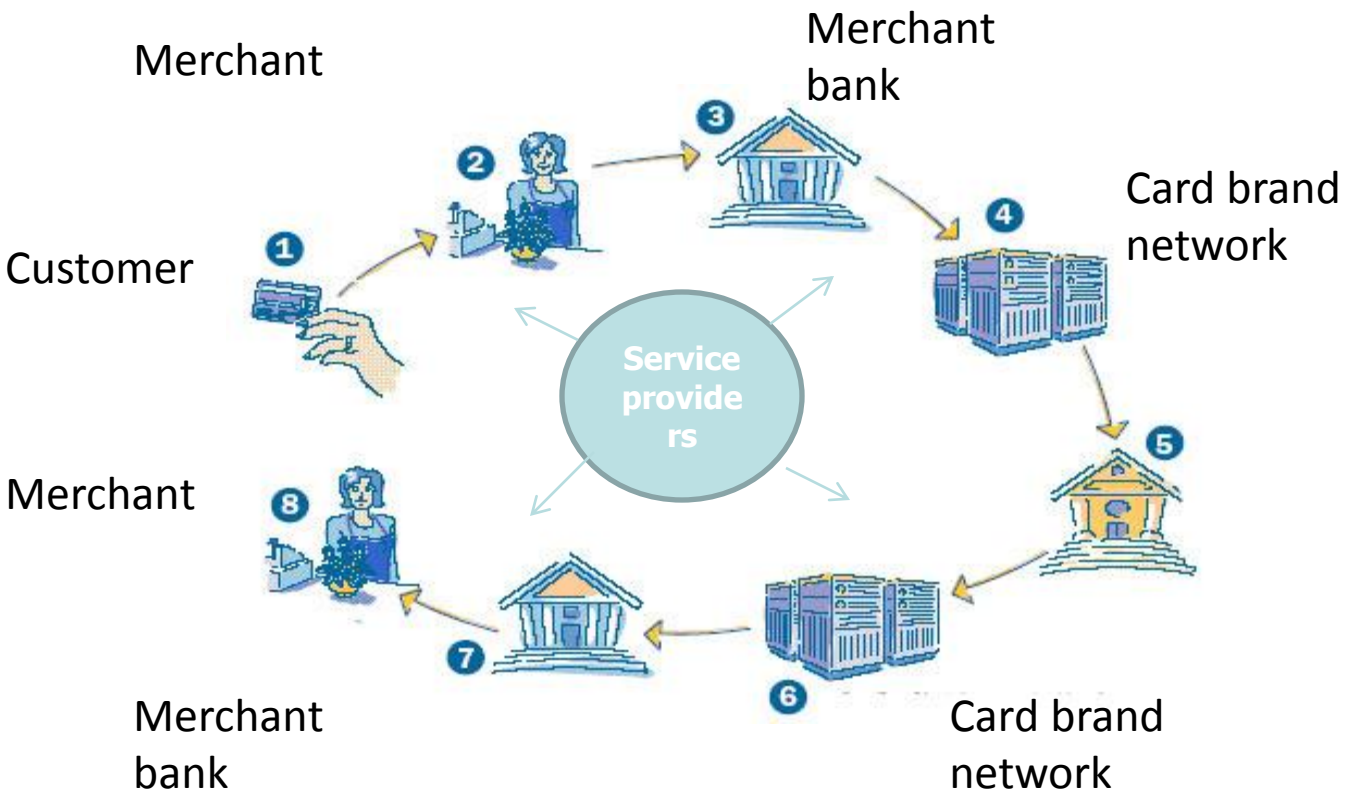
- All five payment brands share equally in the Council's governance, have equal input into the PCI Security Standards Council and share responsibility for carrying out the work of the organization.

- The PCI DSS requirements for merchants, vendors and security consulting companies, and the Council's certification and merchant support services, all created to mitigate data breaches and prevent payment cardholder data fraud.

- Note that enforcement of compliance with the PCI DSS and determination of any non-compliance penalties are carried out by the individual payment brands and not by the Council. Any questions in those areas should be directed to the payment brands.

PAYMENT CARD BRANDS

PLAYERS OF PAYMENT CARD INDUSTRY



DIGITAL DOZEN

- **Build and Maintain a Secure Network**

  Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
  Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

- **Protect Cardholder Data**

  Requirement 3: Protect stored cardholder data.
  Requirement 4: Encrypt transmission of cardholder data across open, public networks.

- **Maintain a Vulnerability Management Program**

  Requirement 5: Use and regularly update anti-virus software.
  Requirement 6: Develop and maintain secure systems and applications.

- **Implement Strong Access Control Measures**

  Requirement 7: Restrict access to cardholder data by business need-to-know.
  Requirement 8: Assign a unique ID to each person with computer access.
  Requirement 9: Restrict physical access to cardholder data.

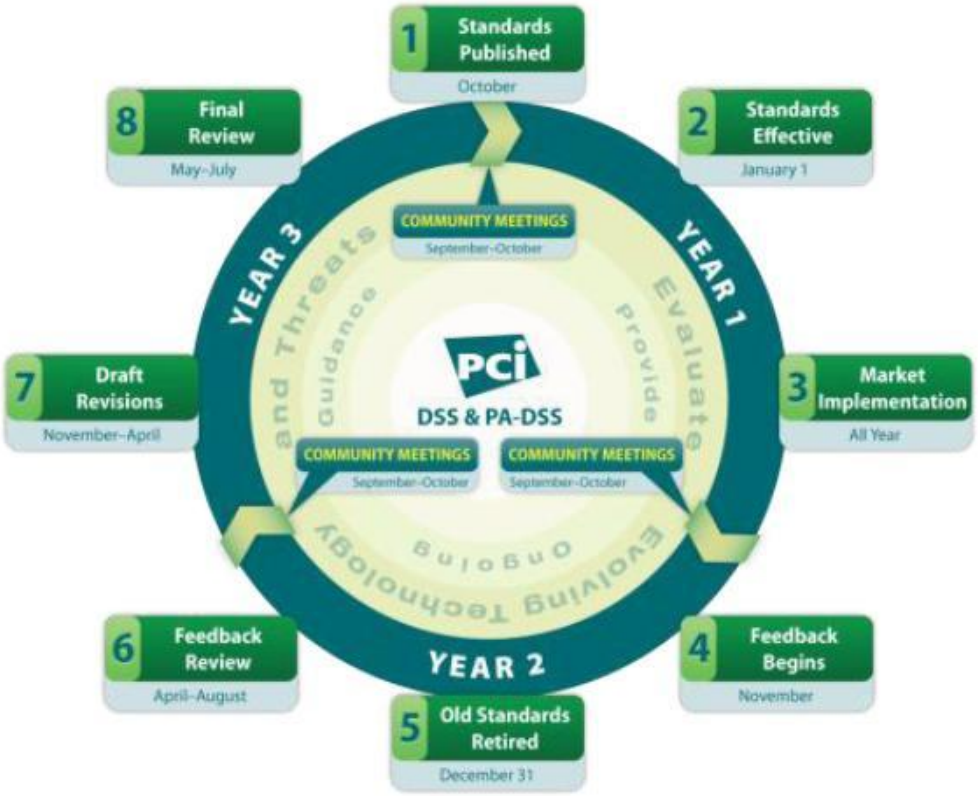
- **Regularly Monitor and Test Networks**

  Requirement 10: Track and monitor all access to network resources and cardholder data.
  Requirement 11: Regularly test security systems and processes.

- **Maintain an Information Security Policy**

  Requirement 12: Maintain a policy that addresses information security.

PCI DSS LIFE CYCLE



Changes in V2.0

Summary of Changes

Classification 119

Additional Guidance – Explanatory 15

Evolving Requirements 2

Effective date

1.1.2011	All Assignments covered under v2.0.
31.12.2010	Assignments Commenced on or before this date under V1.2.1
31.12.2011	Last date for completing assignments under V1.2.1

EVOLVING REQUIREMENTS

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities

- Vulnerabilities identified are required to be risk rated.
- Only of enhancement value upto June 30,2012.
- Mandatory effective from July 1,2012.
- New requirement: 6.5.6 Test Procedures to address high risk vulnerabilities

Additional Guidance

- Requirement 1 extends to :
  Components providing functionality

- Examples of insecure services extended

- Methods of preventing disclosure of private IP addresses.

- Use of virtualization

- Process for detecting wireless Access Points

- Risk assessment methodologies

- “Personnel” instead of “Employees”

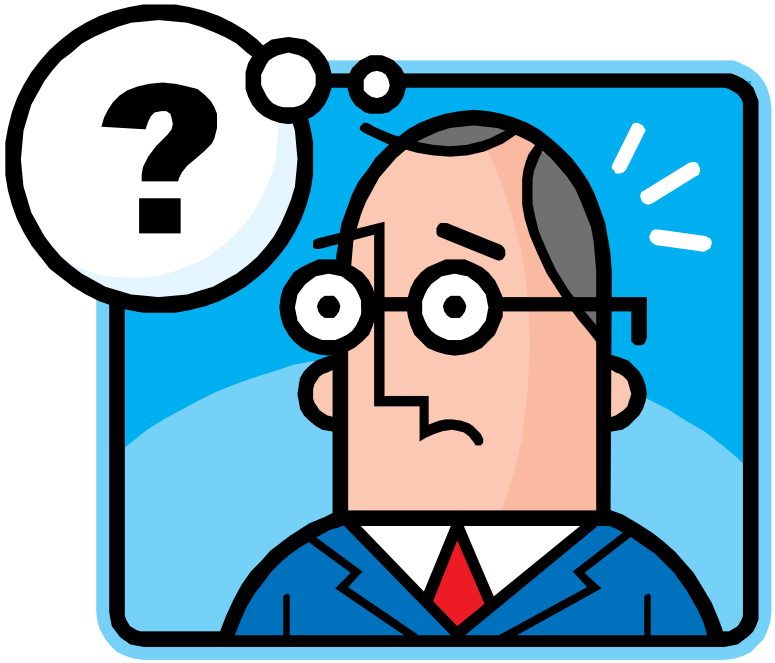
Clarifications-Additions

- Additions
- Deletions
- Relocations

Clarifications – PA DSS Alignment

Requirement 8 :Unique user id – To align with PA-DSS requirement 3.2-POS to have access to one card number at a time.

Q & A




THANK YOU