Foundstone Professional Services A DIVISION OF McAFEE McAfee

Top 10 PCI Concerns

Jeff Tucker

Sr. Security Consultant,

Foundstone Professional Services

About Jeff Tucker

- QSA since Spring of 2007, Lead for the Foundstone's PCI Services
- Security consulting and project management for national and international firms.
- Engagement experience includes:
  - Development of security mgt. programs, policies and procedures.
  - Risk and compliance assessments
  - Remediation planning for global corporations.
- Technical engagements include:
  - Vulnerability assessments
  - Penetration, application and database security testing.
- Jeff.Tucker@foundstone.com

Top Ten PCI Concerns

1. Scope Management
2. Auditing and Logging
3. Understanding Compensating Controls
4. Virtualization
5. Proof of Compliance
6. Stored Cardholder Data
7. Developing Secure Software
8. Compliance Validation
9. Outsourcing
10. Incident Response

Payment Card Industry

Introduction to PCI

Foundstone Professional Services A DIVISION OF McAFEE

McAfee

An Introduction to the PCI Council

- The PCI Council was formed in 2006 to safeguard customer information. Members include:
  - American Express
  - Discover Financial Services
  - JCB International
  - MasterCard Worldwide
  - Visa International

PCI Security Standards Council™

An Open Global Forum

- Rules of Participation:
  - Pay annual dues
  - For additional information, link to the following URL: https://www.pcisecuritystandards.org/pdfs/participating_organization_rules.pdf
- How to join:
  - Application URL address: https://www.pcisecuritystandards.org/participation/membership_application.shtml

Secure Card Data (Account Data)?

► Card Data includes:

1. Cardholder Data.
2. Sensitive Authentication Data.

What is Card Data (Account Data)?

- Card Data includes:

  1. Cardholder Data.

  2. Sensitive Authentication Data.

Cardholder Data	**Sensitive Authentication Data**
• Credit Card Number AKA (PAN) Primary Account Number	• Full magnetic stripe data or equivalent on a chip
• Cardholder Name	• CAV2/CVC2/CVV2/CID
• Expiration Date	• PINs/PIN blocks
• Service Code	

Top Ten PCI Concerns

1 - Scope Management

Managing scope facilitates compliance and reduces risks and costs

Scope Management – Key Issues & Impact

- Under-scoping
  - PCI scope environment is not accurately defined:
    - Systems left out of scope do not process cardholder data, BUT connected to card-processing environment.
  - This is common with Level 2, 3 & 4 merchants.
  - Easily identified when independently audited by card companies.
- Organizations have not effectively segmented their PCI or card data systems.

Scope Management – Recommendations

- Understand your enterprise architecture.
- Education – ensure security design. authorities understand the impact of PCI and any changes to PCI requirements.
- Isolate card-processing environments:
  - At network layer.
  - At application layer.
  - At process layer.

PCI Scope Criteria

- The Cardholder Data Environment (CDE) is comprised of people, processes and technology that store, process, transmit or handle ‘card data’.

PCI Scope Criteria

- The Cardholder Data Environment (CDE) is comprised of people, processes and technology that store, process, transmit or handle ‘card data’.
- Systems that can make (initiate) an IP connection to the CDE, even though they may not have access to ‘card data’ or have administrative access to system components.

PCI Scope Criteria

- The Cardholder Data Environment (CDE) is comprised of people, processes and technology that store, process, transmit or handle ‘card data’.
- Systems that can make (initiate) an IP connection to the CDE, even though they may not have access to ‘card data’ or have administrative access to system components.
- Groups of people that have access to ‘card data’ or administrative access to system components.

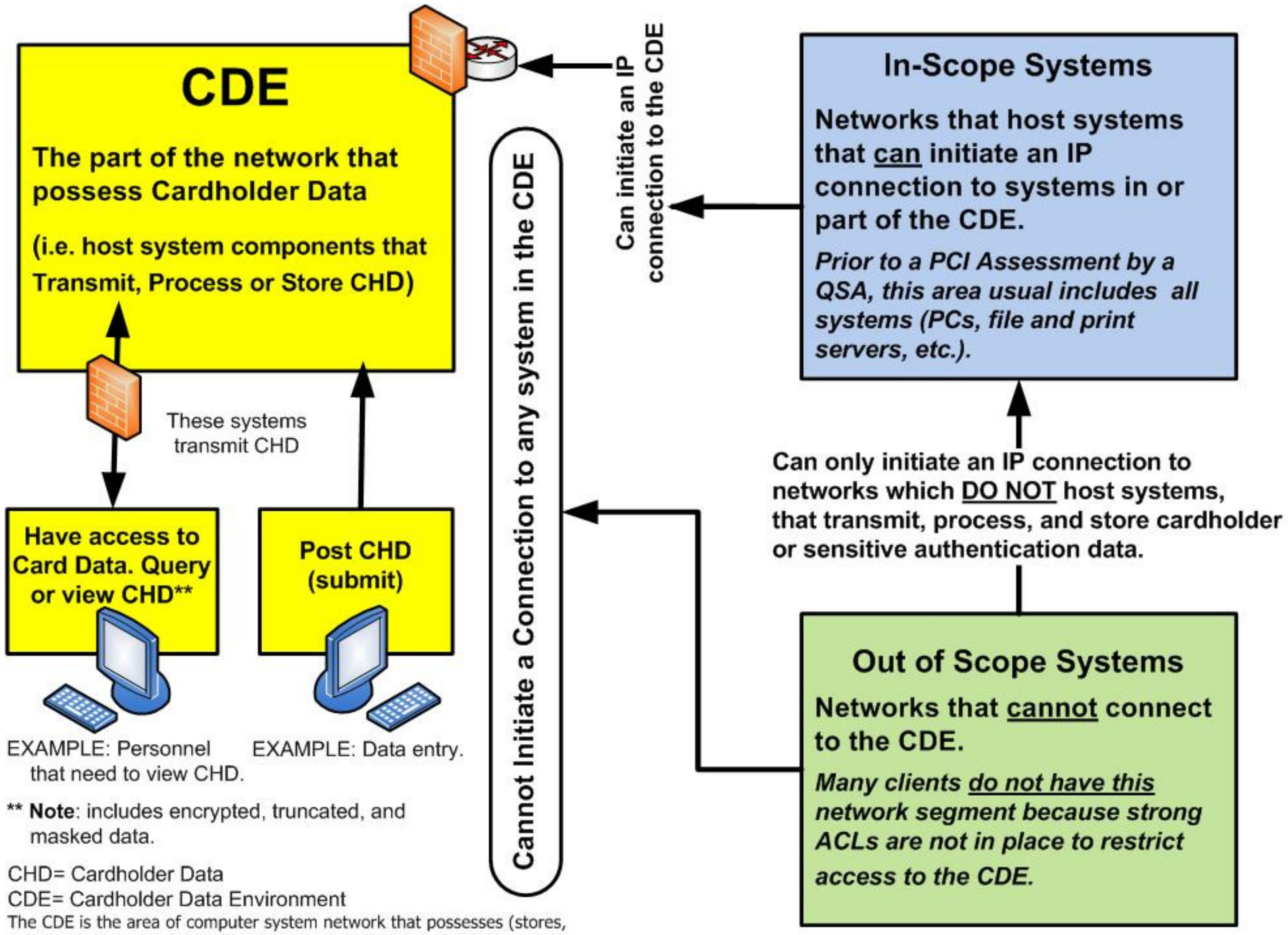
PCI Scope Criteria

- The Cardholder Data Environment (CDE) is comprised of people, processes and technology that store, process, transmit or handle ‘card data’.
- Systems that can make (initiate) an IP connection to the CDE, but do not have access to ‘card data’ or have administrative access to system components.
- Groups of people that have access to ‘card data’ or administrative access to system components.
- Processes that involve the handling of ‘card data’.

PCI Scope Criteria

- The Cardholder Data Environment (CDE) is comprised of people, processes and technology that store, process, transmit or handle ‘card data’.
- Systems that can make (initiate) an IP connection to the CDE, but do not have access to ‘card data’ or have administrative access to system components.
- Groups of people that have access to ‘card data’ or administrative access to system components.
- Processes that involve the handling of ‘card data’.

PCI Scope Criteria



CDE

The part of the network that possess Cardholder Data

(i.e. host system components that Transmit, Process or Store CHD)

These systems transmit CHD

Have access to Card Data. Query or view CHD**

Post CHD (submit)

EXAMPLE: Personnel that need to view CHD.

EXAMPLE: Data entry.

** **Note**: includes encrypted, truncated, and masked data.

Cannot Initiate a Connection to any system in the CDE

Can initiate an IP connection to the CDE

In-Scope Systems

Networks that host systems that <u>can</u> initiate an IP connection to systems in or part of the CDE.

Prior to a PCI Assessment by a QSA, this area usual includes all systems (PCs, file and print servers, etc.).

Can only initiate an IP connection to networks which <u>DO NOT</u> host systems, that transmit, process, and store cardholder or sensitive authentication data.

Out of Scope Systems

Networks that <u>cannot</u> connect to the CDE.

Many clients <u>do not have this</u> network segment because strong ACLs are not in place to restrict access to the CDE.

CHD= Cardholder Data

CDE= Cardholder Data Environment

The CDE is the area of computer system network that possesses (stores, processes, or transmits) cardholder data or sensitive authentication data, and those systems and segments directly attached to the CDE or support card data processing, storage, or transmission.

Foundstone Professional Services A DIVISION OF McAFEE

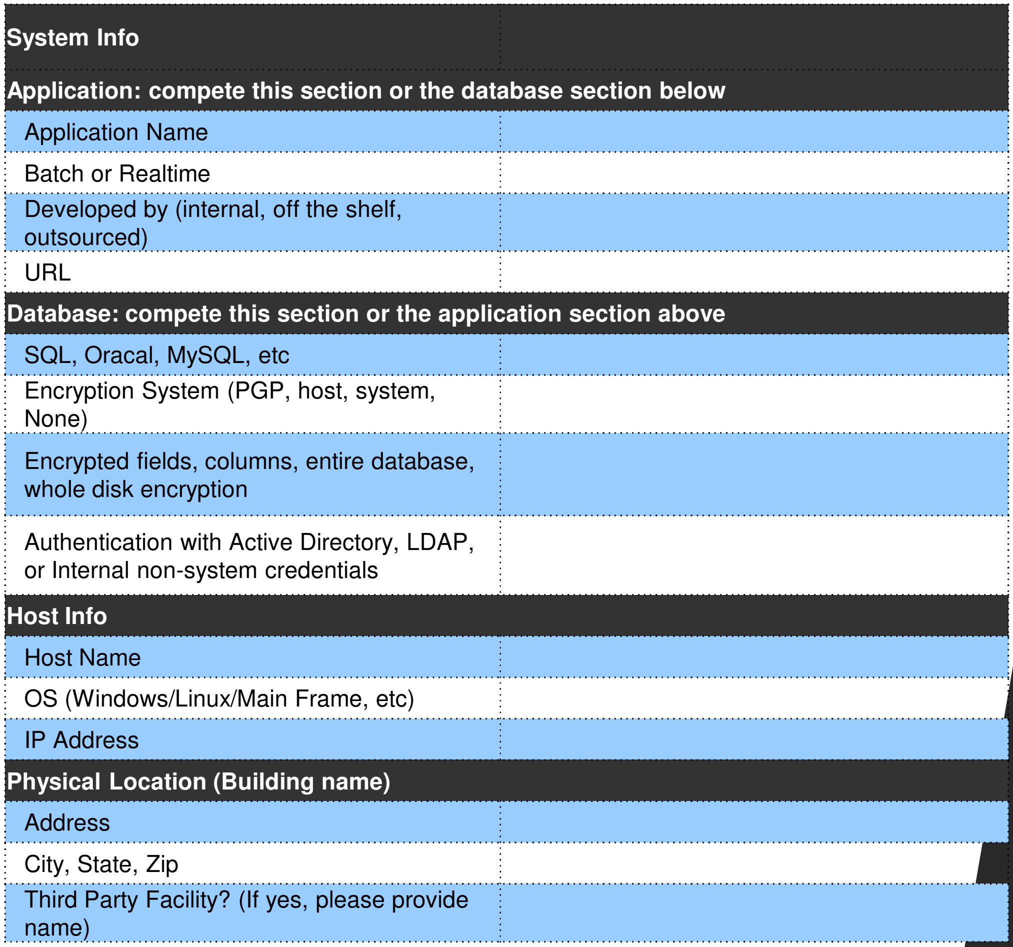
McAfee

www.foundstone.com

Scope Management

Inventory & Scoping:

- ► Is cardholder data stored, processed, or transmitted?
- ► Where is the cardholder data stored?
- ► What systems process or transmit cardholder data ?



System Info	
Application: compete this section or the database section below	
Application Name	
Batch or Realtime	
Developed by (internal, off the shelf, outsourced)	
URL	
Database: compete this section or the application section above	
SQL, Oracal, MySQL, etc	
Encryption System (PGP, host, system, None)	
Encrypted fields, columns, entire database, whole disk encryption	
Authentication with Active Directory, LDAP, or Internal non-system credentials	
Host Info	
Host Name	
OS (Windows/Linux/Main Frame, etc)	
IP Address	
Physical Location (Building name)	
Address	
City, State, Zip	
Third Party Facility? (If yes, please provide name)	

2 - Auditing and Logging

Central Event Correlation

Foundstone Professional Services A DIVISION OF McAFEE

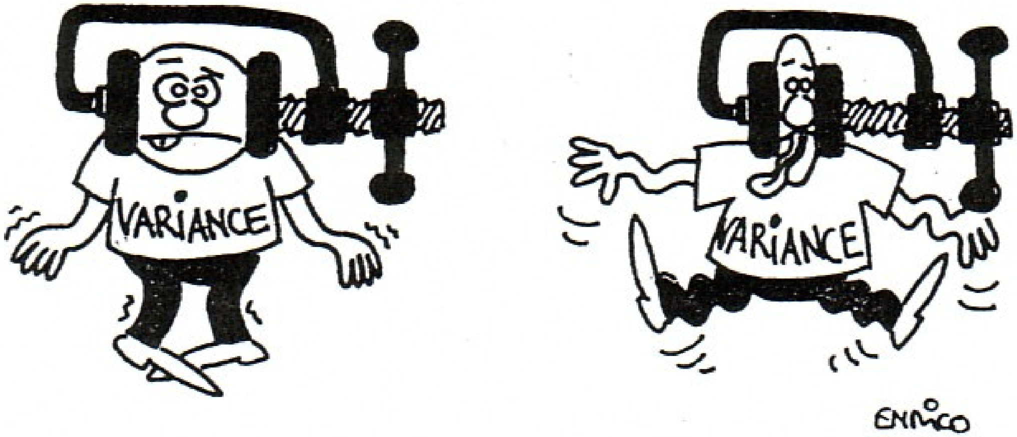
McAfee

Auditing and Logging – Key Issues & Impact

- Auditing and logging are conducted as an Ad-Hoc solution.
  - Lack of centralized and/or enterprise framework.
- Smaller organizations heavily dependent on manual review of log data.
  - Logs are not adequately reviewed.
- Organization that have a great log management system, fail to establish adequate logging parameters.
  - Only log successful system logon events.

Auditing and Logging - Recommendations

- System administrator should have a strong understanding of PCI-DSS requirements to ensure they have configured system correctly.
- Establish a formal process for auditing and log management (i.e., a framework).
- Establish central log management system:
  - Effectively segmented from rest of the network.
  - Establish separation of duties. Sys Admins should not manage the central log management system.
- Automate log review process with central event correlation systems:
  - Auto log parsing.
  - Auto report generation.
  - Alerting function using multiple channels.
    - Email, Pager, or Text to cell phone.



3 - Understanding Compensating Controls

When required controls cannot be deployed, counter measures can be used

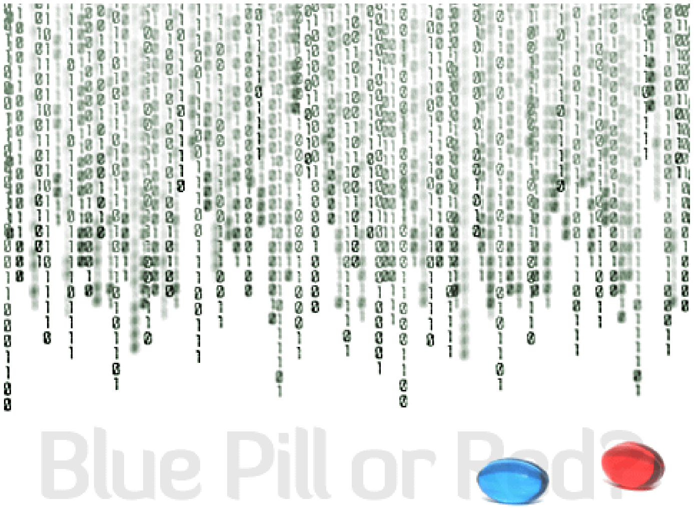
Foundstone Professional Services A DIVISION OF McAFEE McAfee

Compensating Controls – Key Issues & Impact

- ►Limited knowledge of the purpose and the requirements of compensating controls.
- ►Belief that the implementation of a compensating control removes the requirements from future assessments.
- ►Formal risk analysis not performed:
  - ■ Controls selected based on convenience, rather than security.
  - ■ Easily identified when independently audited by card companies.

Compensating Controls - Recommendations

- Work closely with your acquirer and QSA to validate your compensating controls (CCs).
  - Some QSA Companies have a more mature process.
  - Some reject all CCs.
  - Some realize that they are a vital component for compliance.
- Once compensating controls are accepted, implement a plan to meet the original requirement.
  - Or CCs will need annual validation.
- Perform a formal risk assessment.
  - Based on industry standards such as NIST 800-30, OCTAVE, ISO 27005.
- Select compensating controls based on risk assessment.



4 - Virtualization

Virtualization – Key Issues & Impact

- Virtualization and Segmentation
  - A hypervisor in an environment.
  - A hypervisor hosting any PCI systems is a PCI environment.
  - All systems in a PCI Environment are in scope.
- Security and Virtualization
  - Many administrators do not configure the hypervisor securely.
  - Access rights are Over-Assigned on Hypervisors
- Virtual Machines (VMs) typically do not follow the same change management processes
- VMs are easy to copy and install
  - Large increase in "Rogue" installations.

Virtualization – Recommendations

- Understand the security architecture of the products you are using.
- For PCI systems, use a dedicated hardware server.
- Ensure all systems (including VMs) are hardened to a high security level standard.
- Increase VM security training.
- Ensure that planning has included the whole team; including the network, security, and storage teams.
- Ensure security assessments on all servers (including VMs) are conducted periodically.
- Monitor for "Rogue" VMs on Desktops and Laptops.

5 - Proof of Compliance

Generate reports on compliance activities

Foundstone Professional Services A DIVISION OF McAFEE

McAfee

Proof of Compliance – Key Issues & Impacts

- Lack of documentation:
  - Policies & Procedures
    - (SOP) Security Operating Procedures.
  - Reports documenting required activities
    - Code review documentation/report.
    - Firewall review report.
  - Third-Party compliance reports
- Limited Human Resources:
  - Staff to create and maintain documentation.
  - Costs associated with human resources.
- Limited tools for generating compliance information:
  - Automated tools to investigate potential policy violations.

Proof of Compliance – Recommendations

- Create processes and procedures to include and maintain documentation:
  - Firewall rule set reviews.
  - Risk assessments.
  - Change management (record the process).
  - Security control testing.
- Utilize native features:
  - HIPS and file integrity products.
  - Firewalls, IDS/IPS systems.
- Budget for increased work requirements.

6 - Stored Cardholder Data

Protect stored cardholder data

Stored Cardholder Data – Key Issues & Impact

- More data collected than required.
- Data is retained too long.
- Encrypted data is in-scope unless keys are isolated.
  - http://www.mcafee.com/us/resources/white-papers/foundstone/wp-key-isolation.pdf
- Sensitive authentication data (i.e., magnetic strip data) is collected and stored.
- Data has leaked into other systems.
  - Data encryption is not fully implemented for files and databases containing card account numbers.
- Temporary files lack encryption. Dump files are not purged,
- Encryption requires the establishment of a key management program compliant with 3.5 and 3.6.

Stored Cardholder Data – Recommendations

- Ensure your organization maintains and implements a Card Data retention policy that limits data retention.
- Use strong cryptography:
  - Example AES with at least a 128 bit key.
  - See NIST Special Publication 800-57 parts 1-3, March, 2007.
- Ensure all application are encrypting temporary and/or spooled data files.
- Process to purge temporary files (debug files).
- Protect the data encryption keys by encrypting them with key encryption keys.
  - Implement all requirements in 3.5 and 3.6.
- Use mainstream encryption systems with associated key management.

7 - Develop Secure Software

Develop and maintain secure systems and applications

Developing Secure Software – Key Issues & Impact

- ► Security is not integrated into the Software Development Lifecycle (SDLC) program.
  - ■ Out of the box SLDCs such as Agile are built for speed.
- ► Development staff lack security knowledge and are not aware of the security vulnerabilities and impact of exploits.
- ► Lack of testing tools and/or the knowledge to use these tools.
  - ■ Testing is limited to functional and business requirement testing.

Developing Secure Software – Recommendations

- Incorporate information security throughout the SDLC:
  - Secure Coding standards and education.
- Implement a risk assessment and threat modeling strategy.
- Develop software applications based on industry best practices such as OWASP:
  - Develop and test software in an environment that is separate from production (restricted access to production).
    - Use access controls to enforce the separation.
  - Code reviews must be documented (app, list revisions, issues/corrections, reviewer and developer names, etc.).
  - Test for security issues (can be automated).
  - Testers must not be part of development team.
  - Implement a post test clean up process to remove test accounts and test data.

8 – Compliance Validation Requirements

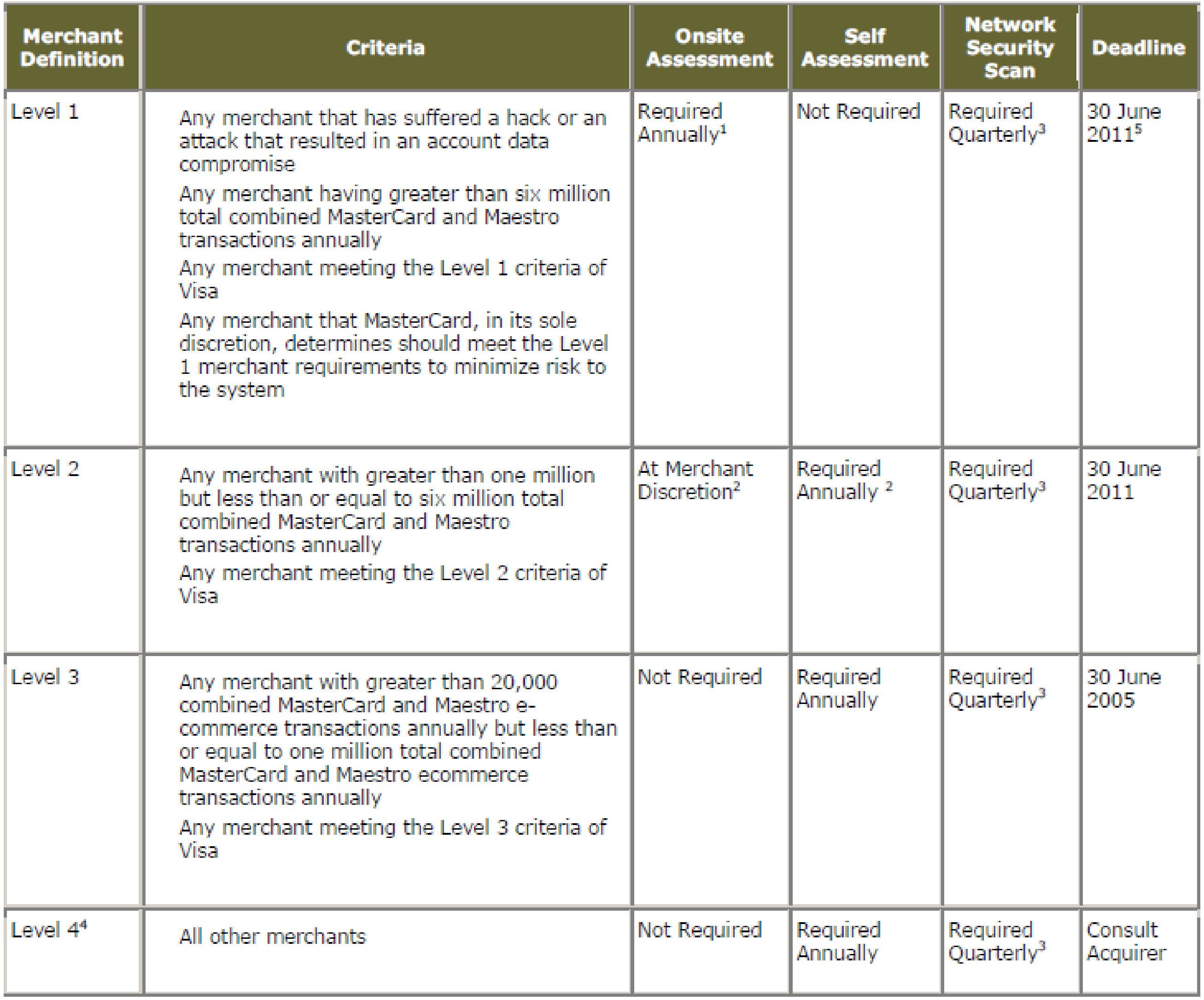
Foundstone Professional Services A DIVISION OF McAFEE

McAfee

Compliance Validation – Key Issues & Impact

- ►Organizations do not know what level of compliance their organization is at.
- ►Most 2-4 level organizations do not understand the PCI DSS requirements, producing an inaccurate Self-Assessment survey.
- ►Many 3-4 level organizations do not understand that they must comply with all applicable PCI DSS requirements regardless of level.

MasterCard Compliance Validation



Merchant Definition	Criteria	Onsite Assessment	Self Assessment	Network Security Scan	Deadline
Level 1	Any merchant that has suffered a hack or an attack that resulted in an account data compromise Any merchant having greater than six million total combined MasterCard and Maestro transactions annually Any merchant meeting the Level 1 criteria of Visa Any merchant that MasterCard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system	Required Annually[1]	Not Required	Required Quarterly[3]	30 June 2011[5]
Level 2	Any merchant with greater than one million but less than or equal to six million total combined MasterCard and Maestro transactions annually Any merchant meeting the Level 2 criteria of Visa	At Merchant Discretion[2]	Required Annually [2]	Required Quarterly[3]	30 June 2011
Level 3	Any merchant with greater than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to one million total combined MasterCard and Maestro ecommerce transactions annually Any merchant meeting the Level 3 criteria of Visa	Not Required	Required Annually	Required Quarterly[3]	30 June 2005
Level 4[4]	All other merchants	Not Required	Required Annually	Required Quarterly[3]	Consult Acquirer

9 - Outsourcing

Reducing the Risk

Foundstone Professional Services A DIVISION OF McAFEE McAfee

Outsourcing – Key Issues & impact

- A ‘Service Provider’ is a business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data.
  - This also includes companies that provide services that control or could affect the security of cardholder data.
  - Managed service providers that provide managed firewalls, IDS and other security services as well as hosting providers and other entities.
- Contracts with service providers DO NOT specifically include PCI-DSS compliance as a condition of business.
- Believe that once a cardholder data task has been outsourced, the PCI requirement has been relieved.
- Members, merchants, and service providers must ensure that service provider handling cardholder data on their behalf are PCI-DSS compliant.

Outsourcing – Recommendations

- Maintain and implement policies and procedures to manage service providers.
  - Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
  - Maintain a list of service providers.
  - Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of:
    - Cardholder data the service providers possess.
    - System components that the service provider manages.
    - That services provided will be compliant with the PCI DSS.
  - Maintain a program to monitor service providers' PCI compliance status at least annually.

10 – Incident Response Plan

Policy – Plan - Procedures

Foundstone Professional Services A DIVISION OF McAFEE McAfee

Incident Response Requirements

- Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands.
- Specific incident response procedures.
- Business recovery and continuity procedures.
- Data back-up processes.
- Analysis of legal requirements for reporting compromises (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database).
- Coverage and responses for all critical system components.
- Reference or inclusion of incident response procedures from the payment brands.

Incident Response Recommendations

- ► Maintain and implement policy, plan and procedures.
- ► Assign program responsibilities to a Director level position.
- ► Create a CIRT and assign responsibility to a Manager.
  - ■ Create a triage team consisting of frontline administrators.
  - ■ Establish triage, reporting and escalation procedures.
  - ■ Provide training.
- ► Incorporate system and network monitoring into CIRT notification.
  - ■ Notify CIRT of unauthorized wireless access point detection.
- ► Contract with experts.
- ► Control external communications.

Top Ten PCI Concerns

1. Scope Management
2. Auditing and Logging
3. Understanding Compensating Controls
4. Virtualization
5. Proof of Compliance
6. Stored Cardholder Data
7. Developing Secure Software
8. Compliance Validation
9. Outsourcing
10. Incident Response

Questions

Foundstone Professional Services A DIVISION OF McAFEE

McAfee