



Credit Card Security considerations And the CSU Audit

Greg Dove, Information Systems Audit Manager

AOA Meeting -- January 9, 2012

Presentation Overview

- Brief overview of OUA IT Audit and Auxiliaries
- Summary of PCI Control Environment
- Objective / Scope of PCI Audit
- What the Auditor will be looking for
- Questions

The Data Security Risk is Significant and Therefore Requires Appropriate Controls

- The threat of data compromise is global in scope (Web)
- Many parties are involved in maintaining data security
- The impact of data compromise is widespread financially, legally, and in goodwill exposures
- Data security is a primary risk concern for Members, Merchants, Service Providers, Consumers, and Regulators
- Data security has evolved from an operational problem and financial threat to a significant reputation risk

The Business Case for Security

- Proper security enables a company to meet its business objective by providing a safe and secure environment that helps avoid:
 - Loss of revenue
 - Loss or compromise of data
 - Interruption of business process
 - Legal consequences
 - Damage to customer and partner confidence
 - Damage to reputation
- A more secure retail store also enables easier and safer connectivity with customers and business partners

Auxiliary IT – What we Audit

- The OBJECTIVE of the IT Audit is to:
 - support the financial audit,
 - by focusing on specific areas of technology,
 - that affect financial transaction processing
- An IT Audit may exclude other technology risks present at a campus or auxiliary such as;
 - Confidential/private information (email, HIPPA)
 - Some network vulnerabilities, Voice, Hacker threats
 - Non-financial systems (H/R, non-res alien tax, etc.)

Objectives of IT Audit

- Advise management on technology and process risks
- Assess control measures and test for effectiveness
- Evaluate the “big picture” view of the entire environment, not just a division / departmental view
- Provide opinions, suggestions and recommendations

PURPOSE of AUDIT to Determine:

- What are the system / process controls that management uses to ensure that the desired results are achieved?
- How do we know that we are compliant with government regulations?
- How do we know that all data is identified and securely stored?
- Is validation testing performed regularly?

IT Audit – Risk Based

EXACTLY What is that CRAZY AUDITOR DOING?

- There is no Magic Checklist: IT topics consistent with organization risk and statutory requirements
- The Level of Detail: in certain areas is based on specific technologies used or areas of financial or business risk
- Adapted: each time to allow for changes in regulation, and in technologies and organization
- Originally: began with high-level organizational controls and have been ratcheting down to lower-level process controls through successive tri-annual audits

Vigilance and Oversight of Auxiliary Operations

- Campus Internal Audit: compliance with procedures
- Information Security Office: Campus wide oversight of security issues and training
- Management – Understanding of processes and the impact/benefit of technologies
- Executive – Support for initiatives and assist with oversight and campus-wide roll out.

6-step Approach to Implementing PCI¹

A prioritized implementation approach to assist organizations in understanding how to reduce risk earlier in the compliance process.

1. Remove sensitive authentication data and limit data retention. “if you do not need it, do not store it”
2. Protect the perimeter, internal and wireless networks. points of access into the cardholder data environment (CDE)
3. Secure payment card applications.
 - Applications, application processes and application servers
 - Secure coding practices, application firewalls and Payment Application Standards (PA-DSS)
4. Monitor and control access to your systems.
 - Controls that limit access and provides detection mechanism for unusual activity within the CDE
5. Protect stored cardholder data.
6. Finalize remaining compliance efforts, and ensure all controls are in place. to protect the CDE

¹ PCI Security Standards Council, PCI DSS Prioritized Approach for PCI DSS 2.0, May 2011

The PCI framework is divided into 12 security requirements

Build and Maintain a Secure Network

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

Protect Cardholder Data

3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.

Maintain a Vulnerability Management Program

5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications

Hint: Things Greg might look for

The PCI framework is divided into 12 security requirements

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

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

Maintain an Information Security Policy.

12. Establish high-level security principles and procedures.

Hint: Things Greg might look for

PCI Compliance Vs Validation

- **Compliance** (daily) – Means **adherence** to the standard
 - Applies to every merchant regardless of volume
 - Technical and business practices
- **Validation** (annual) – Verification that merchant (including its services providers) is **compliant with** the standard
 - Based on Level assigned to merchant, per transaction volume
 - Two types of Validation
 - Self-Assessment
 - Certified by a Qualified Security Assessor (QSA)
- **Attestation** – Letter to Visa signed by both merchant and acquirer bank attesting that validation has been performed

Two Components to Validation

- **Annual Assessment Questionnaire**
 - **Required of all merchants** – regardless of level
 - Self-Assessment or performed by Qualified Security Assessor
 - Must not have any “No” answers – it’s Fail or Pass
 - Applies to both technical and business

- **Security Vulnerability Scan - Quarterly**
 - Required for External facing IP addresses
 - Web applications
 - POS Software and databases on networks
 - Applies even if there is a re-direction link to third third-party
 - Must be performed by Approved Scanning Vendor (ASV)
 - Based on Level assigned to merchant, per transaction volume
 - Visa & MC schedules are different, most go by VISA schedule

Hint: Things Greg might look for

What Does Greg Look for?

- Evidence that risks to the process / system / data have been evaluated
- Evidence that management controls have been implemented to ensure the accuracy and integrity of the process / system
- Evidence of compliance with regulations
- Evidence that the process is working as intended by management
- Evidence that staff understand their role in ensure the process is working

Document the Process Flow

- Network Diagram is Required for all systems that *transmit*, store or process transactions, from the merchant system to the processor.
 - Put processing activities on a separate network segment
 - ➔ – Campus network / 4CNET may need to be compliant or follow an encrypted path
- ➔ ▪ All point of entry into the network / system must be identified and protected.
- All Reports, downloads, and receipts must be protected.

Considerations for Paper

- Physical protective measures are required for storing and securing paper transactions.
 - Report distribution controlled and reports physically locked; which is difficult to demonstrate compliance.
 - Transaction detail must be restricted to only authorized persons and must be physically locked.

- A detailed documented process of all printouts and paper copies of transaction detail is required.
 - Difficult to demonstrate compliance without detailed understanding of the flow process
 - Retention requirements must include adequate security provisions

How is the PCI Audit Different from Past?

- More Detailed Focus on Results not Process
- Identify Any NO Responses
- Determine Appropriateness of Assessment Form
- Evaluate the YES Responses and Obtain Evidence of Compliance
- Examine Results of Scans

Discussion and Questions