



PCI Certification Issues

February 2008

Acquirer Systems Conference

Evolution of PCI DSS

- 2000 Visa CISP(USA) and AIS (EU)
- 2000 Mastercard SDP.
- 2004 – Visa, Mastercard, American Express and JCB agree PCI Standard.
 - The objective of PCIDSS compliance is designed to protect the card companies, merchants and consumers from suffering financial and data loss because of unprotected network systems.

Validation Requirements

Group	Tier	Volumes	Validation Required
Service Providers	1	Any payment gateway regardless of volume.	On-site Audit Annually Network Scan Quarterly
	2	Service providers processing more than 1 million transactions annually.	On-site Audit Annually Network Scan Quarterly
	3	Service providers processing less than 1 million transactions annually.	Self Assessment Annually Network Scan Quarterly
Merchants	1	Greater than 6 million transactions per year	On-site Audit Annually Network Scan Quarterly
	2	Between 150,000 and 6 million transactions per year.	Self Assessment Annually Network Scan Quarterly
	3	20,000 to 150,000 transactions per year.	Self Assessment Annually Network Scan Quarterly
	4	All other merchants.	Self Assessment recommended Annually Network Scan recommended Quarterly

Practical Pitfalls

- The Human Element
 - Ongoing Security Awareness Training
- Un-documented procedures
 - Usage of spreadsheets in a company.
- Third Party Service Providers
 - Connected Entities Program required to ensure all entities are PCI Compliant.
- The “annual audit syndrome”
- Poorly behaved third party applications
 - Payment Application Security Standard

PABP

- Payment Application Best Practices
 - Launched in 2005
 - List of validated payment applications published monthly since January 2006.
 - PABP to move to the Payment Application Security Standard (PASS) and will be administrated through the PCI SSC.
 - Applicable to any third party payment application that is involved in authorisation and settlement of credit/debit card transactions.
 - Is not applicable to dumb terminals, database or web server software. Does apply to applications built on DB & Web.

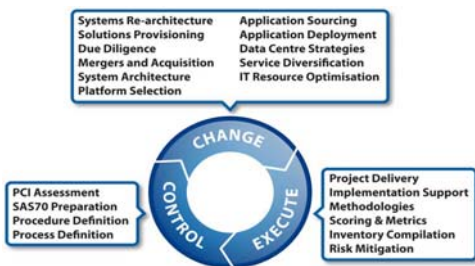
Checklist for Review

- Are all relevant third party applications on the PABP/PASS list?
- Are you sure that all entities in the transaction chain are PCI certified and audited?
- Are all current staff aware of their data security obligations?
- Is any card data (normally resident in a database) extracted to be further analysed?
- What happens sensitive data files after transmission/receipt?

Checklist for Review

- Is PCI Compliance a year round activity?
- Are all new processes and procedures are vetted against the PCI Data Security Standard?

Services Provided



Further Information

- Knowledge Base at
 - <http://www.o-cgroup.com>
- PCI Validation Requirements
 - <http://www.o-cgroup.com/pci-requirements.php>
