Protect 2013

1263 - PCI: delivering governance through SSA

Omar Aldahir, Sr. Fortify Consultant

Revenue Recognition approval required

In order for your presentation to be shown at HP Protect 2013, this form must be filled out and each deck must be approved by the Rev Rec team.

Presentation will be given by Omar Aldahir HP speaker __HP customer __HP partner

Products mentioned in presentation	Version #	Date first shipped	Discussing future?	Pre-announcement?
Example Product	1.2b	Last year	NO	If yes, who is approver?

Pointperson for questions or issues for HP Software from Rev Rec is Philippa Mars, project email alias rrpm@hp.com .

1263 - PCI: delivering governance through SSA

Objectives

PCI-DSS and PA-DSS Overview

PCI-DSS and PA-DSS Mapping

PCI Failure

Grafting PCI to an SSA Program

Governing an effective program

Enforcing Governance

1263 - PCI: delivering governance through SSA

Understanding PCI compliance (refresher)

What is PCI-DSS

PCI DSS has never been a compliance program. It is a standard baseline for assessing compliance that the five major card brands (Visa, MasterCard, American Express, Discover, and JCB)

1263 - PCI: delivering governance through SSA

PCI Failure

Governance

- security should not only be built like a staircase of combined measures
- should be mutually dependent on each other
- Information security should not be regarded as a technical issue
- business and governance challenge that involves adequate risk management, reporting, and accountability
- addressed at the highest levels of the organization, but also adopted at the lowest level

1263 - PCI: delivering governance through SSA

Governance

Alignment

Expand PCI compliance from its primary domain into larger overall governance of the greater IS domain.

Link to organizational strategic goals (IS manager challenge)

Move away from the silo approach and implementation

Securing cardholder data

1263 - PCI: delivering governance through SSA

Understanding Policy

Compliance Does Not Equal Security

- Compliance is not a checklist of policies.
- A Benchmark for integration (people, policies, technology, and processes)
- Must be monitored and updated regularly
- Passing complicate can still leave you vulnerable

1263 - PCI: delivering governance through SSA

Understanding Policy

Security Does Not Equal Compliance

- Well designed security solution won't mean you'll pass compliance
- However implementing either or both reduces risk

1263 - PCI: delivering governance through SSA

Understanding PCI DSS and PA-DSS requirements

Relationship between PCI-DSS and PA-DSS

The Payment Application Data Security Standard (PA-DSS) is derived from the requirements of the PCI DSS

Use of a PA-DSS compliant application by itself does not make an entity PCI DSS compliant, since that application must be implemented into a PCI DSS compliant environment and according to the PA-DSS Implementation Guide provided by the payment application vendor (per PA-DSS Requirement 13.1).

– PCI Standards Council

1263 - PCI: delivering governance through SSA

Understanding PCI DSS and PA-DSS requirements

Just a few of the ways payment applications can prevent compliance

1. Storage of magnetic stripe data and/or equivalent data on the chip in the customer's network after authorization;
2. Applications that require customers to disable other features required by the PCI Data Security Standard, like anti-virus software or firewalls, in order to get the payment application to work properly; and
3. Vendors' use of unsecured methods to connect to the application to provide support to the customer.

– PCI Standards Council

1263 - PCI: delivering governance through SSA

Understanding PCI DSS and PA-DSS requirements

PCI DSS Software Compliance

1. Displaying of sensitive information being processed or transmitted by the application
2. Storing of sensitive data within the application

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	yes
	Cardholder Name	Yes	Yes	No
	Service Code	Yes	Yes	No
	Expiration Date	Yes	Yes	No
Sensitive Authentication Data	Full Magnetic Stripe Data	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

1263 - PCI: delivering governance through SSA

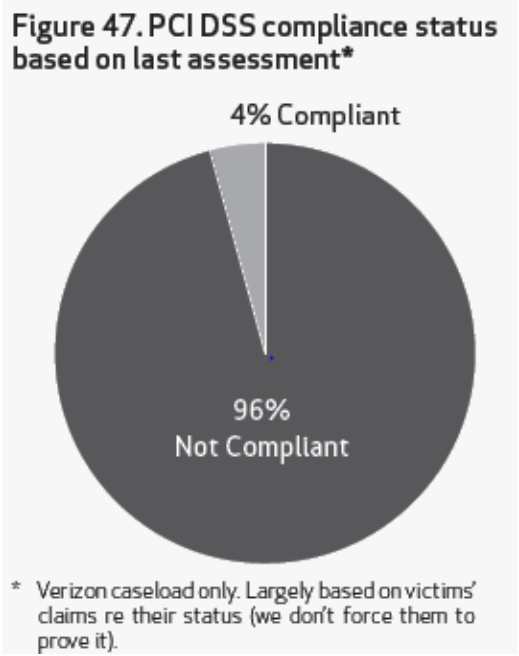
PCI Failure

PCI DSS Software Compliance

compliance != security

96% of breach victims were not compliant as of their last assessment

Verizon 2012 DBR



1263 - PCI: delivering governance through SSA

PCI Failure

PCI DSS Software Compliance

- Overall, organizations both large and small seem to struggle the most with requirements 3, 7, 10, and 11.
- Interestingly, when looking at the numbers on a year-over-year basis we see mixed progress:
    1. Improved (x5)—Requirements 1, 2, 6, 7, and 9
    2. Declined (x4)—Requirements 3, 5, 8, and 11
    3. Remained the same (x3)—Requirements 4, 10, and 12

Verizon 2012 DBR

1263 - PCI: delivering governance through SSA

PCI Failure

PCI DSS Software Compliance

Cost of annual audits averages $225,000 per year for the largest merchants. Excluding technology, operating, and staff costs, the world's largest acceptors of credit cards (also known as Tier 1 merchants) are spending an average of $225,000 on auditor expenses. 10 percent of these businesses are spending $500,000 or more annually on PCI auditors

.

Verizon 2012 DBR

1263 - PCI: delivering governance through SSA

PCI Failure

PCI DSS Software Compliance

2008 Level 1 Merchants (6 million or > transactions per year) spent 3.38m to obtain compliance (McCoy 2009)

Still 79% received citations for failing to protect stored data (First Data 2009)

1263 - PCI: delivering governance through SSA

PCI Failure

Breaches

2006 at TJX Company Inc
2008 Hanford Bro's
2009 Dept. of Veteran Affairs

As of August 21, 2013, the ITRC has reported 385 breaches for 2013

How many unreported!!!

1263 - PCI: delivering governance through SSA

Understanding Policy

RISK

- Subjective (What's acceptable to One not necessary acceptable to others)
- Goal is to mitigate risk not manage it, however difficult
- Reality is you can only hope to manage it.
- Balancing expectations and costs vs. reparations

1263 - PCI: delivering governance through SSA

Understanding Policy

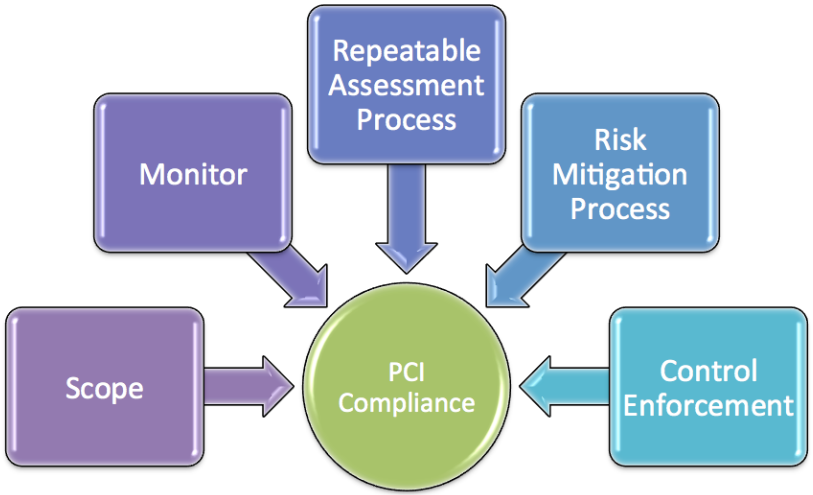
Focus

- Protect cardholder data.
- Focus on non-technical issues
- Include basic IT policies, procedures, and practices, that minimize IT threats
- Proper governance is a key to success

1263 - PCI: delivering governance through SSA

Posture

Changing Posture



1263 - PCI: delivering governance through SSA

Understanding Policy

Mapping

- Scope
- Establish a SSA Program around applications
- Assess Risk
- Enforce

1263 - PCI: delivering governance through SSA

Mapping ISO 27001 and ISO 23034

PCI DSS [1]	ISO 27001 [10]
1. Install and maintain a firewall configuration to protect data.	**A10**.6. Network Security Management
	A11.4. Network Access Control
2. Do not use vendor–supplied defaults for system passwords and other security passwords	**A10**. Communications and operations management
	A11. Access Control
	A12. Information systems acquisition, development and maintenance
3. Protect stored data	**A10**. Communications and operations management
	A12. Information systems acquisition, development and maintenance
	A15. Compliance
4. Encrypt transmission of cardholder data and sensitive information across public networks.	**A10**. Communications and operations management
	A11. Access Control
5. Use and regularly update anti-virus software	**A10**.4. Protection against malicious and mobile code
6. Develop and maintain secure systems and applications.	**A10**. Communications and operations management
	A11. Access Control
	A12. Information systems acquisition, development and maintenance
7. Restrict access to data by business need to know.	A8.1.1. Roles and responsibilities A8.3.3. Removal of access rights
	A11. Access Control
8. Assign a unique ID to each person with computer access.	A8. Human Resources security
	A10. Communications and operations management
	A11. Access Control
9. Restrict physical access to cardholder data.	A8. Human Resources security
	A9. Physical and Environmental Security
	A10. Communications and operations management
10. Track and monitor all access to network resources and cardholder data.	**A10**. Communications and operations management
	A11. Access Control
11. Regularly test security systems and information security management systems with all controls specified in accordance with systems and processes.	**A10**. Communications and operations management
	A12. Information systems acquisition, development and maintenance
12. Maintain a policy that addresses information security.	All [12]

Open Software Assurance Maturity Model		ISO/IEC 27034									
		Normative Framework							Application Security Risk Assessment	Provisioning and Operating theApplication	Application Security Audit
Function	Security Practice	Business context	Regulatory context	Technological context	Application specifications repository	Roles, responsibilities andqualifications	Application security control library	Life cycle reference model			
Governance	Strategy & Metrics	•						◆	•		•
	Policy & Compliance	◆	◆				•				◆
	Education & Guidance			◆		◆	•				
Construction	Threat Assessment				•		•		◆		
	Security Requirements				•		◆			◆	
	Secure Architecture			•	•		◆			◆	
Verification	Design Review						◆			◆	
	Code Review						◆			◆	
	Security Testing						◆			◆	
Deployment	Vulnerability Management			•			◆			◆	
	Environment Hardening						◆			◆	
	Operational Enablement				•		◆			◆	

1263 - PCI: delivering governance through SSA

Mapping ISO 27001 and ISO 23034

Filling the Gaps

1263 - PCI: delivering governance through SSA

Example

Legacy Application

- Retrofitting with new features
  - lack of SME
- Middleware (CORBA) initially designed for interoperability
  - lacks security features
- Web Services (popular)
  - may have to tinker with existing code
- AOP (Aspect Oriented Programming)
  - Good benefits with least impact

Thank you

Protect 2013

Security for the new reality