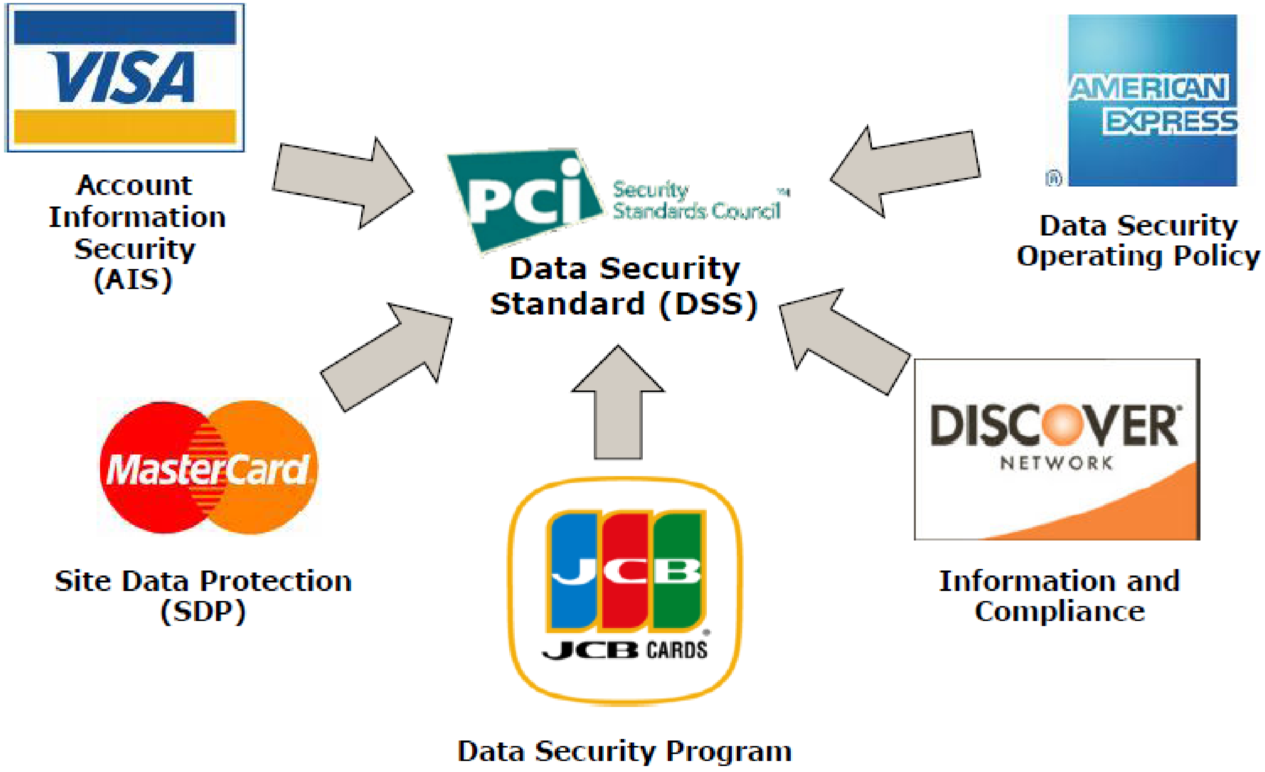
PCI Compliance at The University of South Carolina

Failure is not an option

Rick Lambert PMP
University of South Carolina
ricklambert@sc.edu

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS: "One Standard to Rule Them All"



Account Information Security (AIS)

Data Security Standard (DSS)

Data Security Operating Policy

Site Data Protection (SDP)

Data Security Program

Information and Compliance

Who Must Comply?

Do you….

- Store, process or transmit cardholder data?
  - Point-of-Sale (POS)
  - Mail Order/Telephone Order (MOTO)
  - FAX
  - E-Commerce (website where customer can input their credit card information to complete a transaction)
- Can Affect the Security and/or Integrity of Cardholder Data
- Offer Websites that use PCI Compliant 3rd parties for Processing CHD

IF YOU ANSWER ***YES*** *TO ANY OF THESE QUESTIONS,*
THE PCI DSS APPLIES TO YOU!

PCI Non-Compliance

In the event of a data breach, the card brands can:

- Assess fines
  - Up to $500,000 per brand per breach
- Require that you notify victims
- Require that you pay card replacement costs
- Require that you reimburse fraudulent transactions
- Require forensic investigations be performed by a PCI approved firm
- Require that you validate as a Level 1 merchant (QSA)

Consequences

Direct Costs

- Discovery / Forensics
- Notification costs
- Identity monitoring costs
- Additional security measures
- Lawsuits
- Fines

Indirect Costs

- Loss of customer confidence
- Loss of productivity
- Distraction from core business

10,000 accounts X $200 / account = $2 Million

Plus additional costs if card data is involved

Reputation – Priceless!

PCI DSS: 6 Goals, 12 Requirements

326 individual questions

Goal	Requirements
1. Build and maintain a secure network	1. Install and maintain a firewall configuration to protect data 2. Change vendor-supplied defaults for system passwords and other security parameters
2. Protect cardholder data	3. Protect stored data 4. Encrypt transmission of cardholder magnetic-stripe data and sensitive information across public networks
3. Maintain a vulnerability management program	5. Use and regularly update antivirus software 6. Develop and maintain secure systems and applications
4. Implement strong access control measures	7. Restrict access to data to a need-to-know basis 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
5. Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
6. Maintain an information security policy	12. Maintain a policy that addresses information security

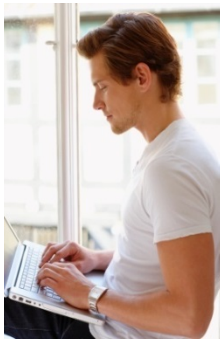
Merchant Levels and Validation

Level	VISA MasterCard DISCOVER NETWORK	AMERICAN EXPRESS
1	• Annual on-site audit (QSA) • Quarterly network scan (ASV)	• Annual on-site audit (QSA) • Quarterly network scan (ASV)
2	• Annual on-site assessment (QSA/ISA) • Quarterly network scan (ASV)	• Quarterly network scan (ASV)
3	• Annual Self-Assessment Questionnaire (SAQ) • Quarterly network scan (ASV)	• Quarterly network scan (ASV)
4	• At discretion of acquirer • Annual SAQ • Quarterly network scan (ASV)	▪ N/A

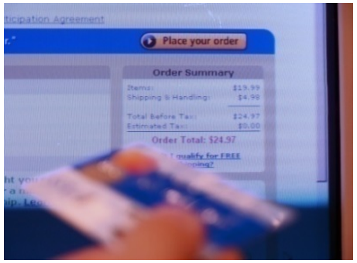
What’s in PCI Scope?

Office Workstations?

Card Swipe Machine?



Student?



Shopping Cart?

Phone Transaction?

Computer Lab?

Defining Your PCI DSS Scope

People, processes and technologies that store, process **or** transmit cardholder data, or that *could affect the security* of those components that do touch the data. Simple, right?

- Workstations
- Servers (web, database, virtual, etc.), and Firewalls, IDS/IPS
- Data Centers & Network closets
- File Cabinets, desk drawers
- "Locked" Doors
- Paper
- People

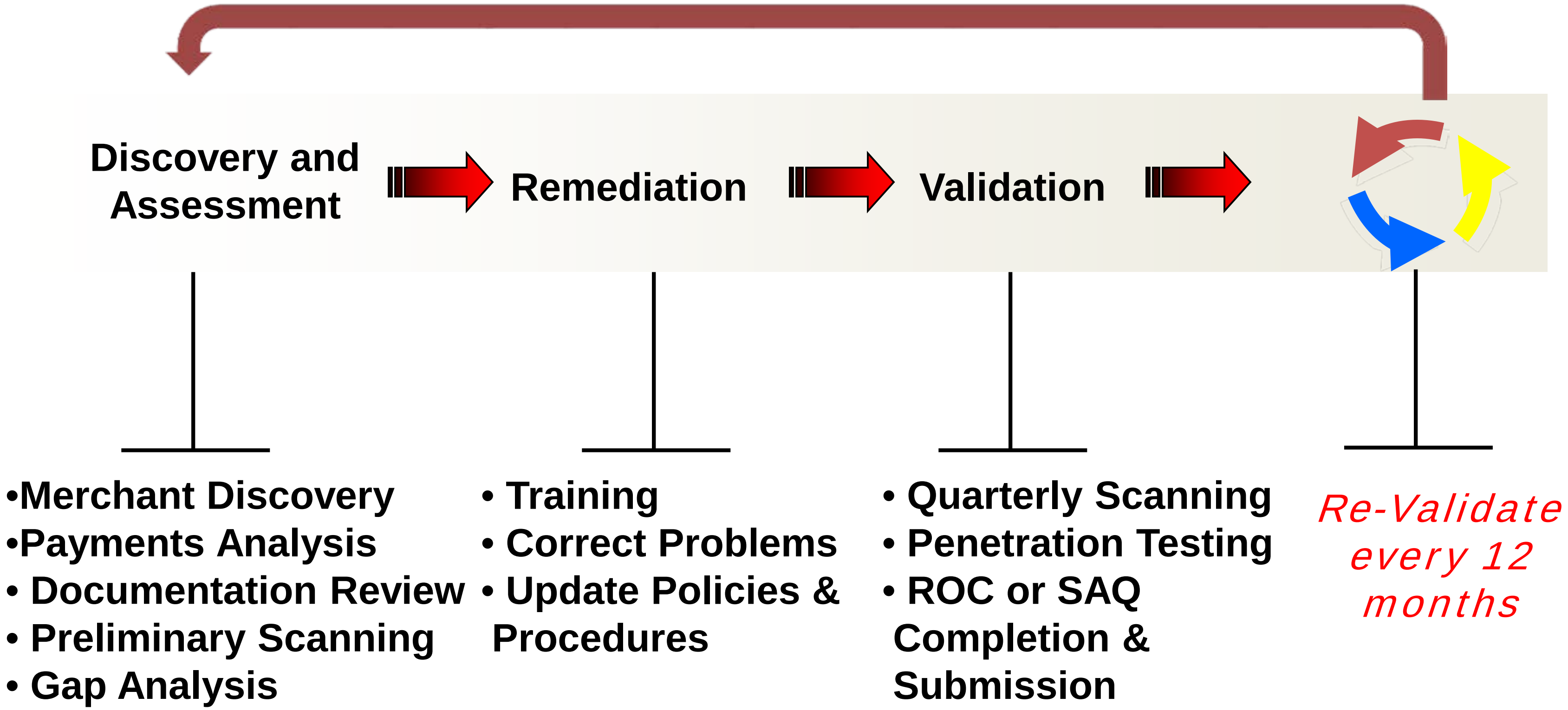
Other Scoping Considerations

- The best first steps are to:
  - Complete and maintain an accurate inventory
  - Complete and maintain an accurate cardholder dataflow diagram
- Once you know exactly where and why cardholder data flows and lives, consider opportunities to streamline, centralize and eliminate
- Segment all card activity from other campus networks
- P2PE holds promise; understand the difference between P2PE and E2EE.

Can I Self Assess?

- Maybe, but you should ask yourself…..
  - Do we fully understand all 326 requirements? Can I relate those to all of the merchants?
  - Do we have the skills to implement the necessary tools and processes?
  - What is my timeline?
  - Do I like my job? ☺

PCI DSS is a Process



Discovery and Assessment → **Remediation** → **Validation** →

- Merchant Discovery
- Payments Analysis
- Documentation Review
- Preliminary Scanning
- Gap Analysis

- Training
- Correct Problems
- Update Policies & Procedures

- Quarterly Scanning
- Penetration Testing
- ROC or SAQ Completion & Submission

Re-Validate every 12 months

Maintaining Compliance

- Maintain PCI team meetings
- Annual Training
- Continued evaluation of systems and services
- Vulnerability scans and penetration testing of systems
- Annual re-assessments
- Ever-changing threat environment
- Web and Internet Solutions

USC PCI Compliance

Project Chartered: May 20, 2010

Project Closed: June 9, 2015

Project Sponsor: University Bursar

Project Objectives

1. Identify the Cardholder Data Environment for the University of South Carolina

2. Provide a PCI Compliant transaction method for all credit card transactions received on behalf of the University of South Carolina

3. Establish the necessary policies, standards and procedures to maintain PCI Compliance for the University of South Carolina

4. Provide an Attestation of Compliance for the University of South Carolina

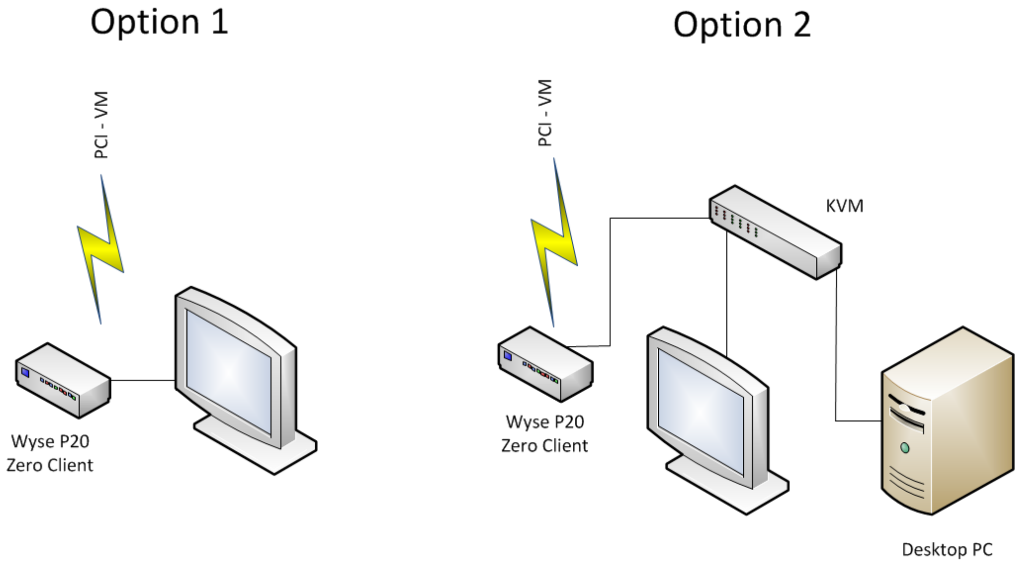
Project Highlights

- Internal Departmental survey was conducted by the project team
  - **700** surveys sent via email for **229** receipting locations in April 2011
  - Survey was completed in September 2011
- USC contracted with CampusGuard and completed initial Gap Analysis in November 2011
  - Completed on campus Gap Analysis of the larger areas
  - Worked with project team to complete remaining areas
- Created PCI Compliant Card Data Environment
  - Utilized a VDI solution with WYSE Zero Clients to access Card Data Environment
  - Contained areas with PCI needs behind individual firewalls
  - Created equipment bundle to supply PCI areas with all hardware and software for devices in the PCI CDE

Project Highlights

- Worked with each area individually to address gaps identified in the analysis
  - Created individual project plans for compliance
  - Created processes and procedures from templates provided by CampusGuard
- Completed all Self Assessment Questionnaires and submitted to CampusGuard for approval
  - Each area was assigned an SAQ according to their business needs
  - Larger areas were assigned multiple SAQs if the business need required
  - All SAQs were then compiled into a single SAQ for the university
- Received Attestation of Compliance on May 28,2015

VDI Solution



Option – 1 Zero client connected to the PCI VM in the PCI Card Data Environment. The image will be hardened to allow access to only those functions necessary to complete a transaction or access the PCI data. No email, Office or internet connectivity available.

Option – 2 Zero client connected to the PCI VM in the PCI Card Data Environment. The image will be hardened to allow access to only those functions necessary to complete a transaction or access the PCI data. No email, Office or internet connectivity available. A KVM switch will allow access the physical PC for daily job functions not associated with PCI data.

Self Assessment Questionnaire Statistics

- USC completed 100 SAQs overall
- USC completed 597 sections overall in the SAQs assigned to departments
- USC responded Yes to 3458 questions overall in the SAQs assigned
- USC responded Not Applicable to 1047 questions overall in the SAQs assigned
  - All NA responses had to be quantified
- USC responded to a total of 4505 questions overall in the SAQs assigned
- Policies and Procedures were created for each department for their everyday business needs as well as Incident Response Plans

Project Successes

- Processes and procedures for maintaining PCI Compliance were formalized
- Risk to the university was reduced
- Repeatable processes were put into place to maintain PCI Compliance
- Awareness levels were raised in the university community
- For the 2014-2015 fiscal year, the University of South Carolina completed **618,946** compliant card transactions
  - This equals approximately **$106,307,071** in compliant card transactions

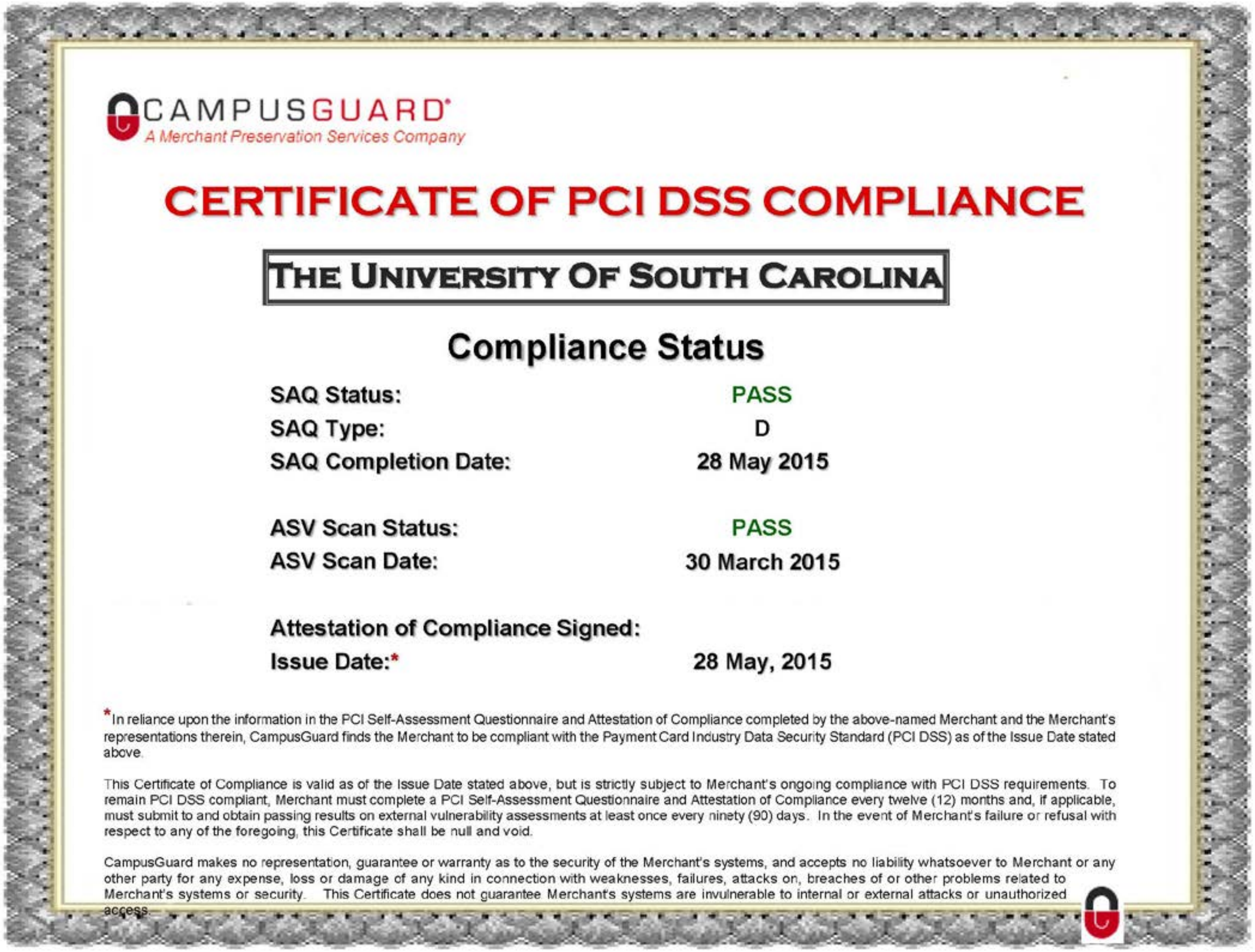
What did we learn?

- Executive support
  - Clear understanding that participation is not optional
  - Must dedicate resources to achieve compliance
- Complete the Self Assessment Questionnaire early
  - Complete SAQ even if it is mostly non-compliant
  - Use the negative responses to create tasks for each area
- Communication
  - Regular communication/meetings to keep the project on track
  - Set dates and assign resources for completion of specific tasks
- Be nice…until it's time to not be nice

Final Thoughts

"You don't get credit for what you started, you get credit for what you finished"

"If you think compliance is expensive- try non-compliance"



CAMPUSGUARD®
A Merchant Preservation Services Company

CERTIFICATE OF PCI DSS COMPLIANCE

THE UNIVERSITY OF SOUTH CAROLINA

Compliance Status

SAQ Status:	PASS
SAQ Type:	D
SAQ Completion Date:	28 May 2015
ASV Scan Status:	PASS
ASV Scan Date:	30 March 2015
Attestation of Compliance Signed:	
Issue Date:*	28 May, 2015

*In reliance upon the information in the PCI Self-Assessment Questionnaire and Attestation of Compliance completed by the above-named Merchant and the Merchant's representations therein, CampusGuard finds the Merchant to be compliant with the Payment Card Industry Data Security Standard (PCI DSS) as of the Issue Date stated above.

This Certificate of Compliance is valid as of the Issue Date stated above, but is strictly subject to Merchant's ongoing compliance with PCI DSS requirements. To remain PCI DSS compliant, Merchant must complete a PCI Self-Assessment Questionnaire and Attestation of Compliance every twelve (12) months and, if applicable, must submit to and obtain passing results on external vulnerability assessments at least once every ninety (90) days. In the event of Merchant's failure or refusal with respect to any of the foregoing, this Certificate shall be null and void.

CampusGuard makes no representation, guarantee or warranty as to the security of the Merchant's systems, and accepts no liability whatsoever to Merchant or any other party for any expense, loss or damage of any kind in connection with weaknesses, failures, attacks on, breaches of or other problems related to Merchant's systems or security. This Certificate does not guarantee Merchant's systems are invulnerable to internal or external attacks or unauthorized access.

Questions