Compliance With The PCI DSS

Today's Agenda

- PCI DSS Introduction
- How are Colleges and Universities Affected?
- How Do You Validate Compliance?
- Best Practices
- Q&A

CampusGuard

- **Full-Service QSA/ASV Firm**
- **We Know Security**
- **Focused Solely on Higher Education**

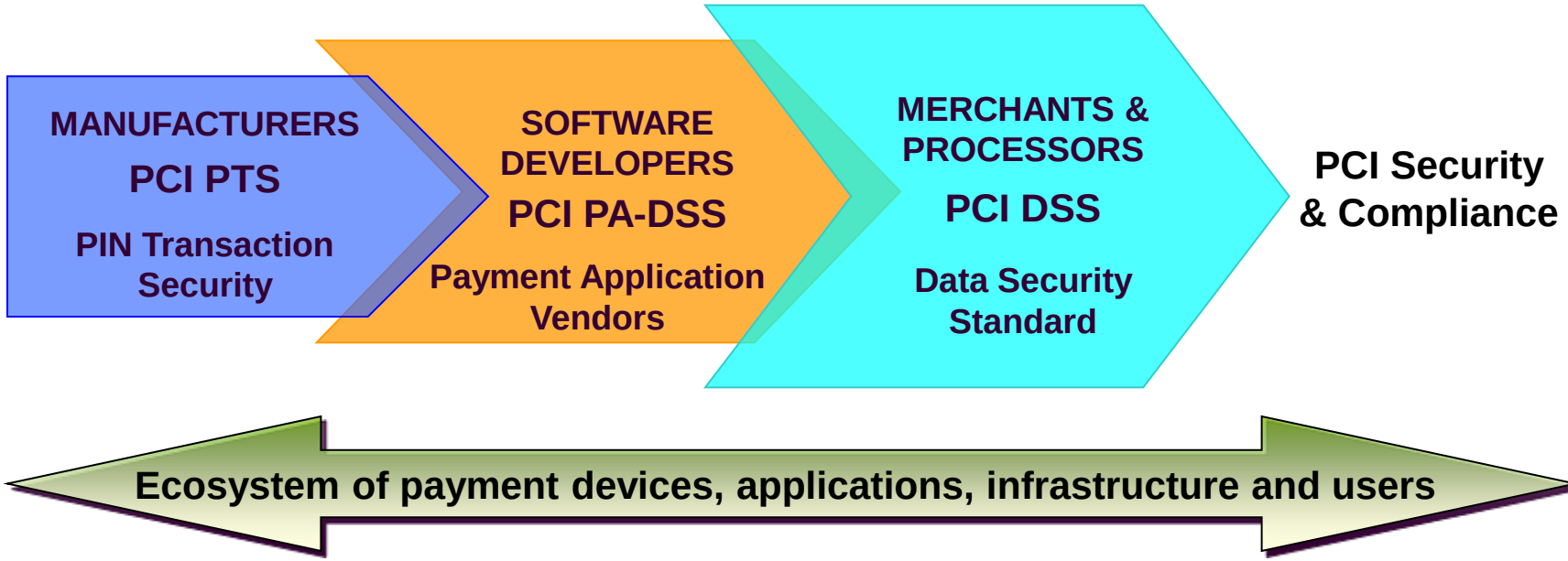
PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council
APPROVED SCANNING VENDOR

The Target Breach

- 40 million customers
- Insider ?
- POS was the vector
- Lessons for all…

PCI…


MANUFACTURERS
PCI PTS
PIN Transaction Security
SOFTWARE DEVELOPERS
PCI PA-DSS
Payment Application Vendors
MERCHANTS & PROCESSORS
PCI DSS
Data Security Standard
PCI Security & Compliance
Ecosystem of payment devices, applications, infrastructure and users

PCI Relationships

PCI Security Standards Council

Responsible for managing the PCI DSS and certifying QSAs and ASVs

Bank

Communicates and educates merchants on PCI DSS and reports compliance status to Card Associations

CREDIT CARD SECURITY

VISA MasterCard DISCOVER NETWORK AMERICAN EXPRESS

Responsible for enforcing and monitoring merchant compliance with the PCI DSS

Merchant

Responsible for safeguarding credit card data and complying with the PCI DSS

Penalties can be **Huge**

- In the event of a breach the bank can make the merchant responsible for:
  - Fines from card associations
    - Up to $500,000
  - + Cost to notify victims
  - + Cost to replace cards
  - + Cost for any fraudulent transactions
  - + Forensics
  - + Level 1 certification

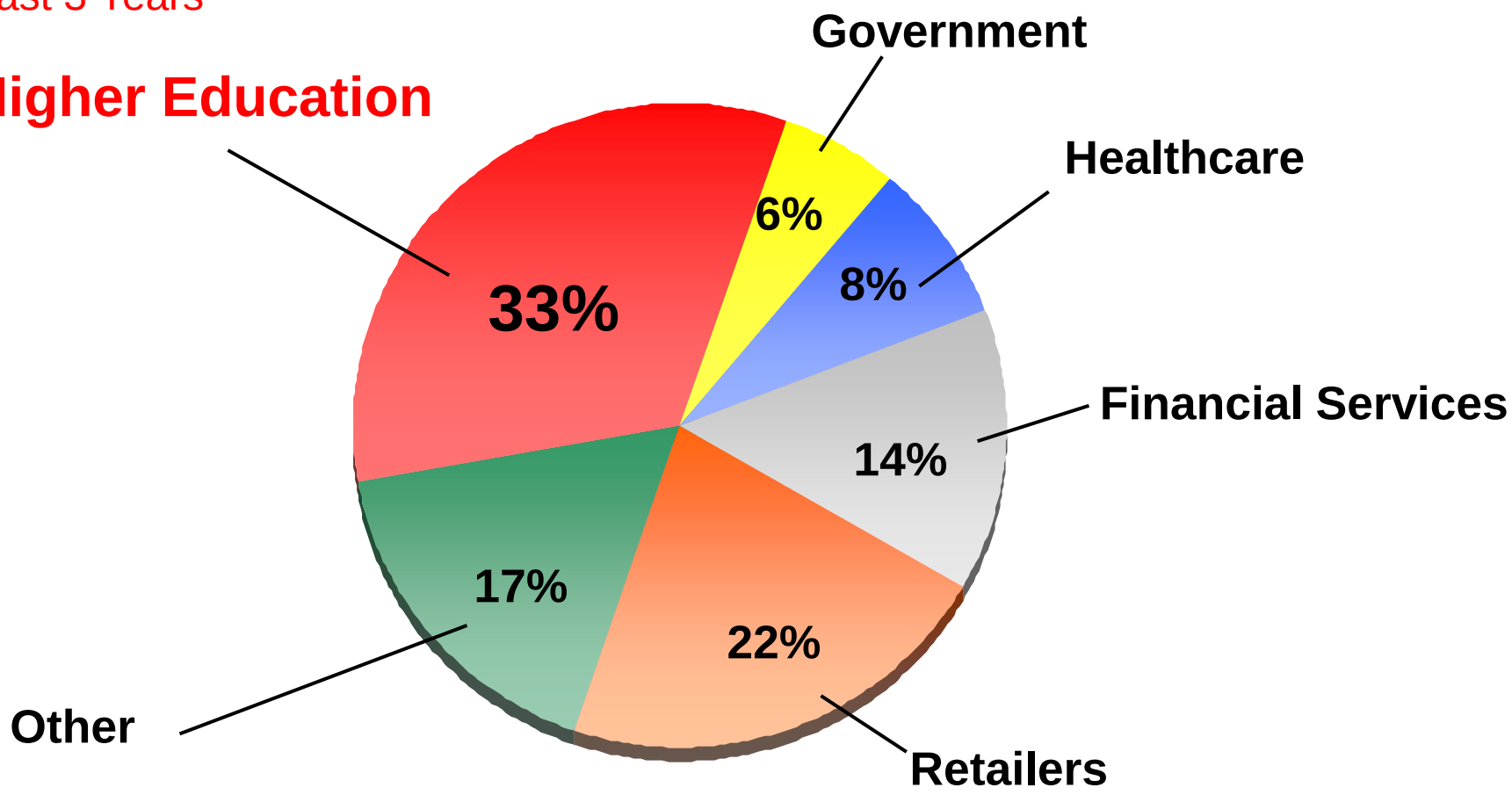
Bad Publicity – Priceless!

How Much Time Left?

- **You are assumed to be compliant NOW!**
- **Banks will be requiring your validation SOON!**

Higher Ed Is Vulnerable

Past 3 Years



Source: Privacy Rights Clearinghouse

Colleges and Universities are like Cities…

A Campus Is A “City"

Challenges for PCI Compliance:

- **Open networks and systems**
- **Scope conversations complex**
- **Overloaded staff**
- **Fiscal constraints**

PCI in Higher Education

What department or functional area at your institution has primary responsibility for PCI compliance?		
Answer Options	**Response Percent**	**Response Count**
Finance (e.g., Treasury, Controller)	58.7%	44
Information Technology	8.0%	6
Responsibility is shared - no single organization has overall responsibility for PCI compliance	33.3%	25
Other (please specify)		13
answered question		**75**
skipped question		**3**

Source: 2012 Treasury Institute PCI Workshop

PCI in Higher Education

Does your institution have written policies for the following?

Answer Options	Yes	No	Don't Know	Response Count
Information security	72	2	4	78
Accepting credit cards	69	5	4	78
PCI compliance	65	9	4	78
Cardholder data access	59	10	9	78
			answered question	78
			skipped question	0

Source: 2012 Treasury Institute PCI Workshop

PCI in Higher Education

How does you institution fund the cost of PCI compliance?		
Answer Options	**Response Percent**	**Response Count**
PCI compliance costs are centrally funded	67.6%	50
Compliance costs are allocated to campus merchants	10.8%	8
Other (please describe how you allocate costs)	21.6%	16

Source: 2012 Treasury Institute PCI Workshop

PCI in Higher Education

Please check the box that describes your institution's PCI compliance:		
Answer Options	**Response Percent**	**Response Count**
We are PCI compliant now	38.6%	27
We expect to validate compliance within 6 months	24.3%	17
We expect to validate compliance in 6-months to 1 year	34.3%	24
We do not have a target date for becoming compliant	2.9%	2

Source: 2012 Treasury Institute PCI Workshop

PCI DSS: 6 Goals, 12 Requirements

Control Objective	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

Level	VISA / MasterCard	American Express
1	> 6 million Visa/MC txns/yr	> 2.5 million transactions/yr
2	1 to 6 million Visa/MC txns/yr	50,000 to 2.5 million txns/yr
3	20,000 to 1 million Visa/MC ecommerce txns/yr	All other Amex Merchants
4	All other Visa/MC merchants	N/A

Most Colleges and Universities

Validation Requirements

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

Self-Assessment Questionnaires

Card-Not Present, All Cardholder Data Functions Outsourced	Imprint Only, No Cardholder Data Storage	Standalone Dial Out Terminal, No Cardholder Data Storage	Payment Application Systems Connected to the Internet	All other methods
SAQ A (11 questions)	**SAQ B (29 questions)**	**SAQ B (29 questions)**	**SAQ C / VT (80/51 questions)**	**SAQ D (286 questions)**

11 ← → **286**

Move as far to the left as possible!

Can I assess myself?

- ***Short answer:*** Maybe (but you probably don't want to)

- ***Long answer:*** You can assess yourself, provided:
  - You follow audit procedures
  - Your acquirer agrees
  - An approved officer (think President or CFO) signs on the "dotted line" (attesting to the veracity of the results)
  - You're absolutely sure you're going to do it right

What's in PCI Scope?

Card Swipe Machine?

Office Workstations?

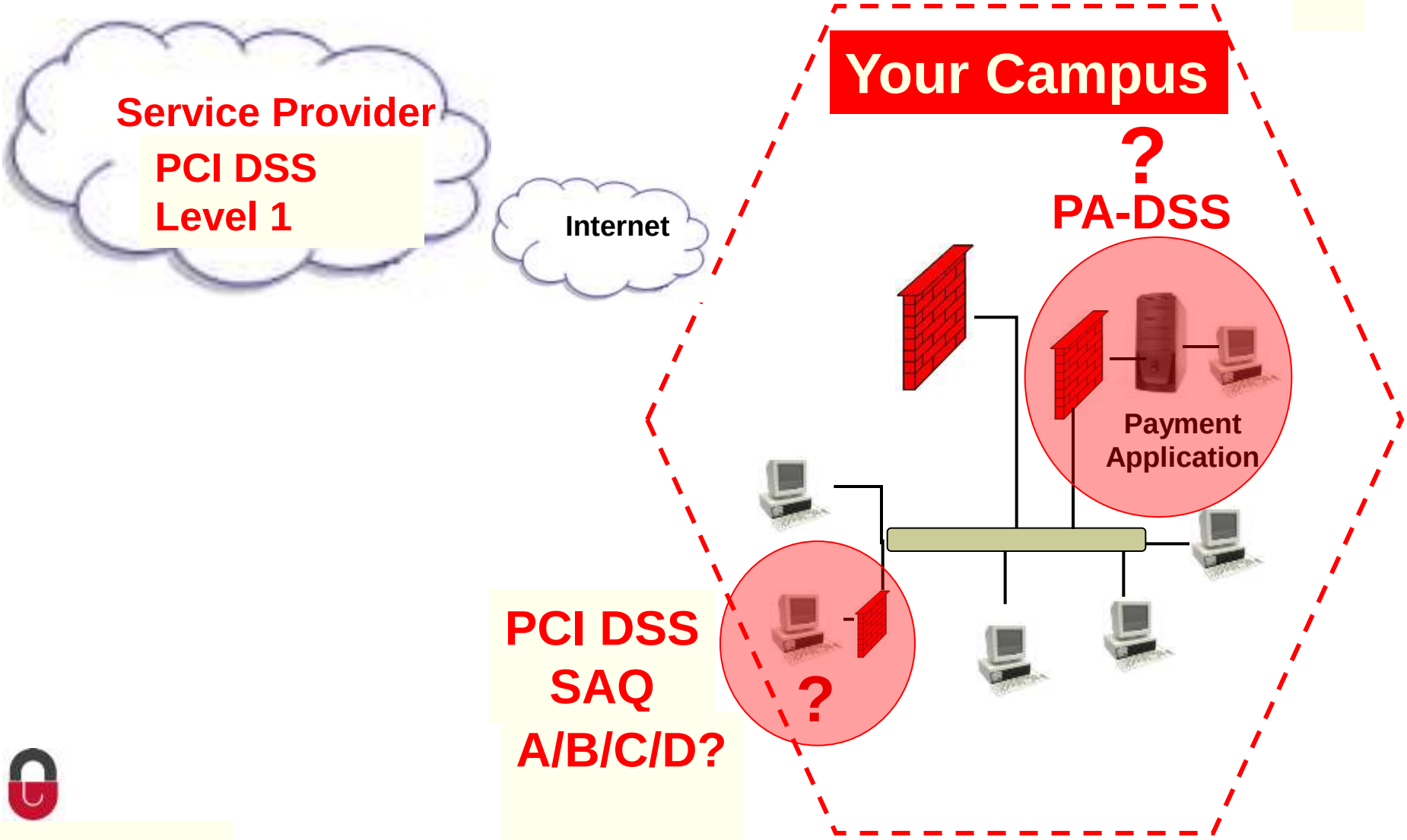
Student in dorm?

Shopping Cart?

Computer Lab?

Phone Transaction?

PCI DSS Assessment

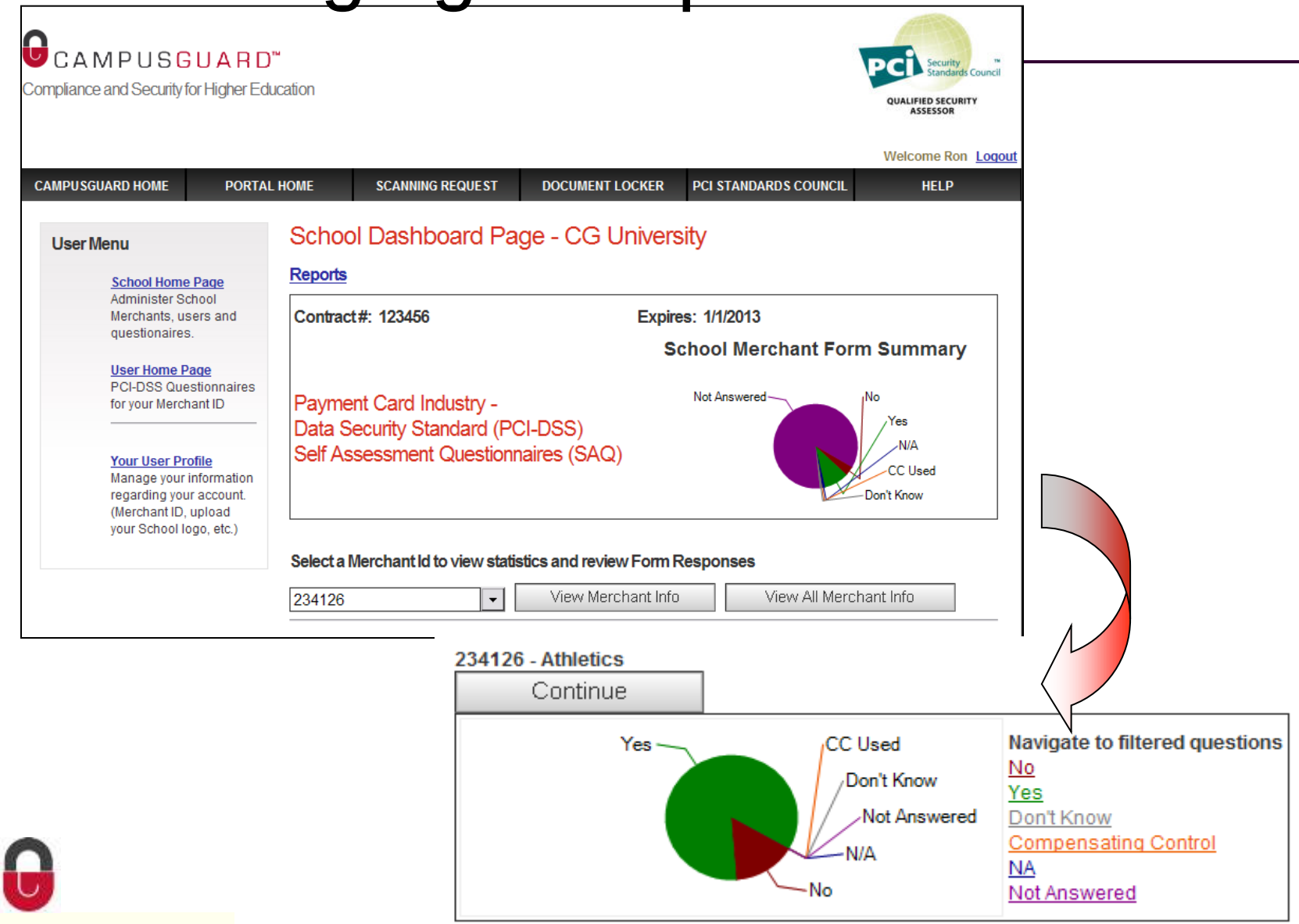


Case Study:

The commercial software was PA-DSS certified, but

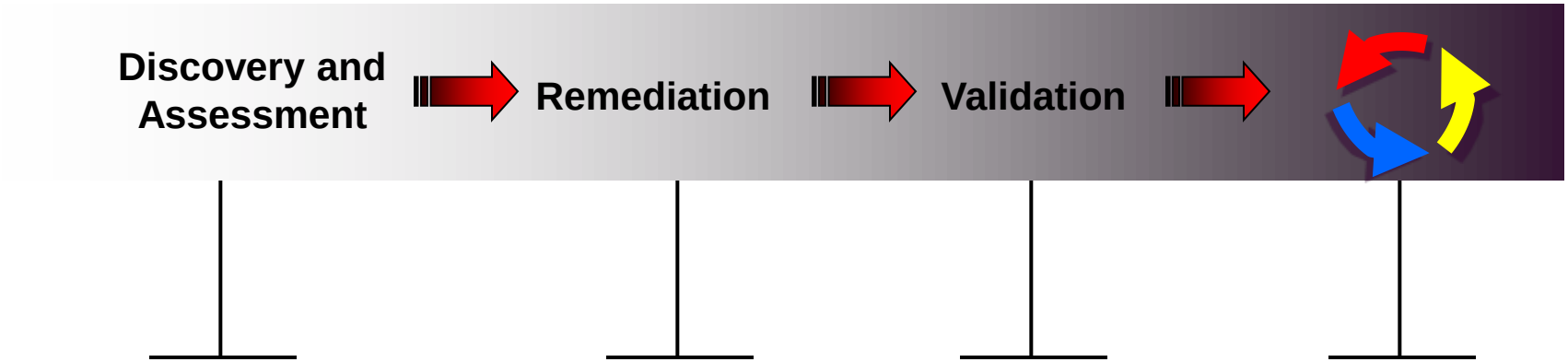
- ~~1~~ – Firewall configuration
- ~~7~~ – Access to system components and cardholder data
- ~~8~~ – Assign unique ID to each person with computer access
- ~~9~~ – Restrict physical access
- ~~11~~ – Regularly test security systems and processes
- ~~12~~ – Maintain a policy that addresses information security

Managing Compliance



Compliance Finish Line!

PCI Compliance



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

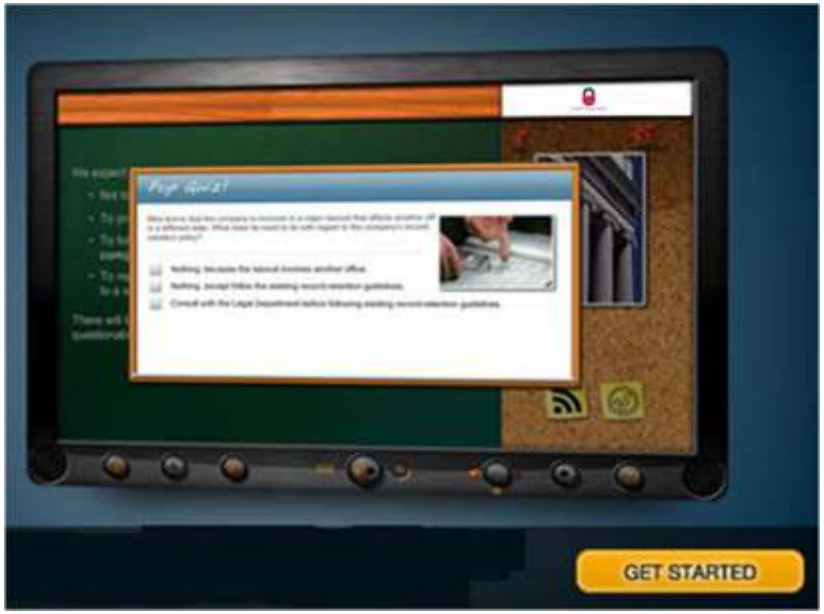
- Correct Problems
- Compensating Controls

- ROC or SAQ Submission

- Quarterly Scanning
- Penetration Testing

Re-Validate every 12 mos

Awareness Training



- PCI DSS
- Red Flags
- HIPAA
- FERPA
- GLBA
- General Info Security
- Identity Theft
- Clery Act
- Title IX

Online Training: PCI DSS

Topics

- An overview of PCI DSS
- PCI DSS objectives and requirements
- Costs of non-compliance
- Sensitive Authentication Data
- Hard-copy storage
- Protecting cardholder information
- Payment card transactions
- Remote access
- Good work practices
- Security incidents
- Restricted computer access
- Restricted physical access
- Tracking and monitoring
- Social engineering

Online Training: Administration

Tracking Tools monitor employee participation in real time

Custom Reports shape data to meet the most comprehensive reporting needs

Scheduled Reports "push" tracking data to administrators

Automated "Reminders" drive high completion rates

Closing Thoughts

- PCI is a journey
- PCI requires partnerships
- Requires perseverance
- Keep the faith

Ron King, CampusGuard
rking@campusguard.com
(972) 964-8884