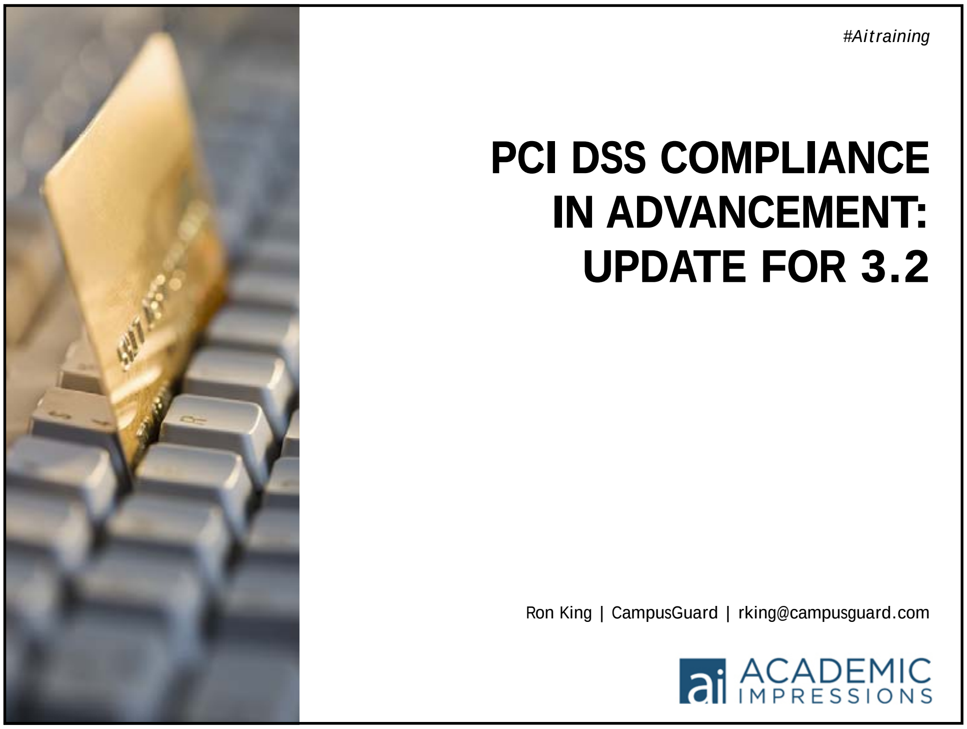
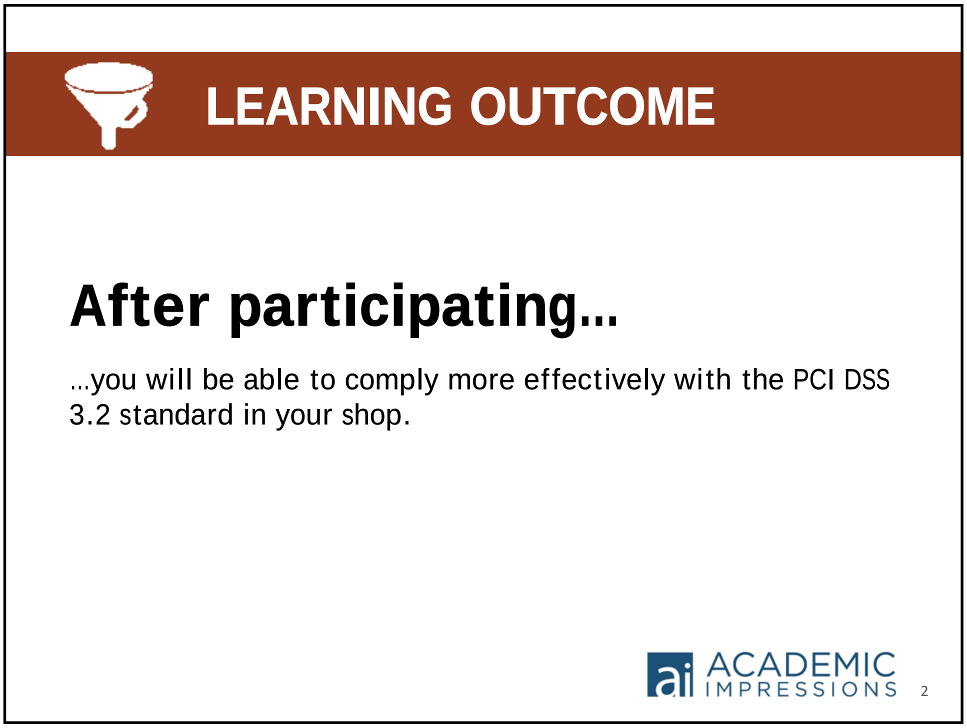


#Aitraining

PCI DSS COMPLIANCE IN ADVANCEMENT: UPDATE FOR 3.2

Ron King | CampusGuard | rking@campusguard.com

ACADEMIC IMPRESSIONS

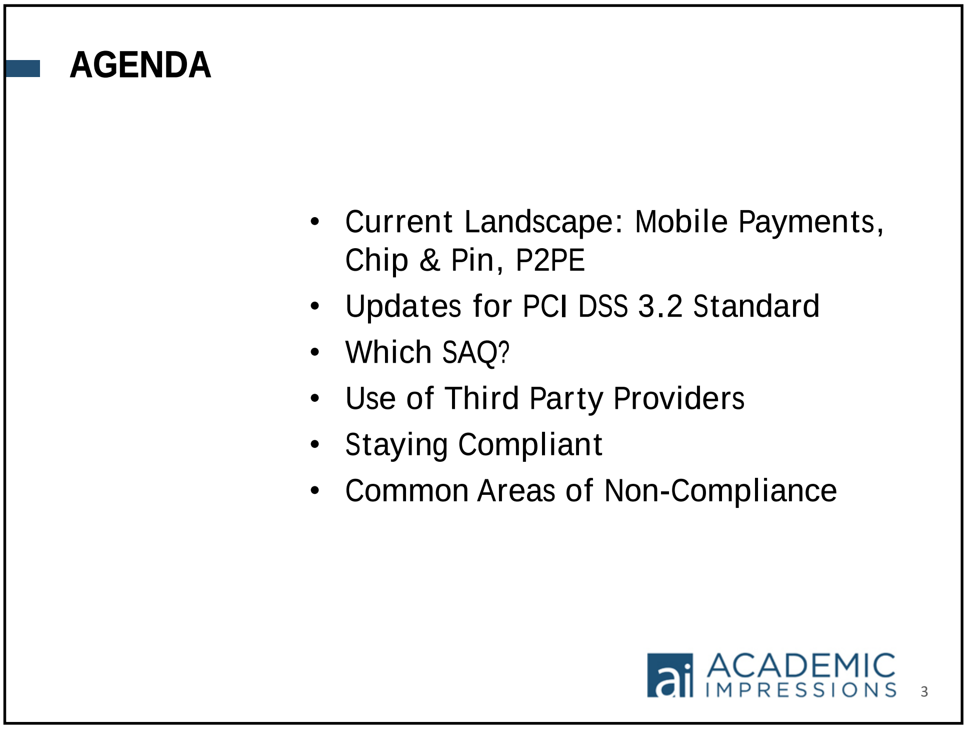


LEARNING OUTCOME

After participating…

…you will be able to comply more effectively with the PCI DSS 3.2 standard in your shop.

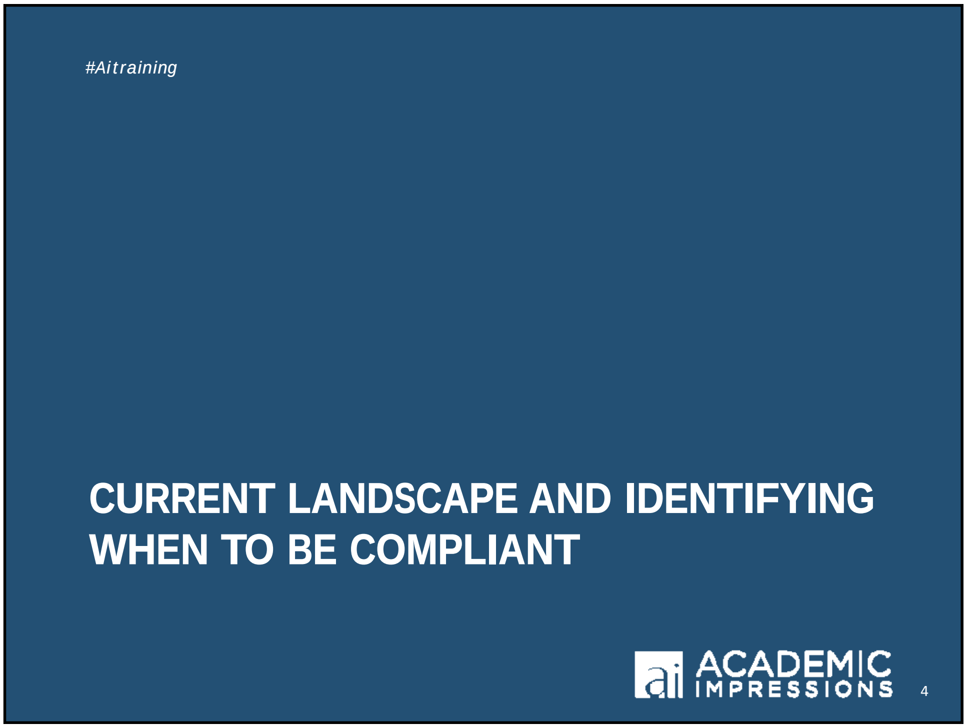
ACADEMIC IMPRESSIONS 2



AGENDA

- Current Landscape: Mobile Payments, Chip & Pin, P2PE
- Updates for PCI DSS 3.2 Standard
- Which SAQ?
- Use of Third Party Providers
- Staying Compliant
- Common Areas of Non-Compliance

ACADEMIC IMPRESSIONS 3



#Aitraining

CURRENT LANDSCAPE AND IDENTIFYING WHEN TO BE COMPLIANT

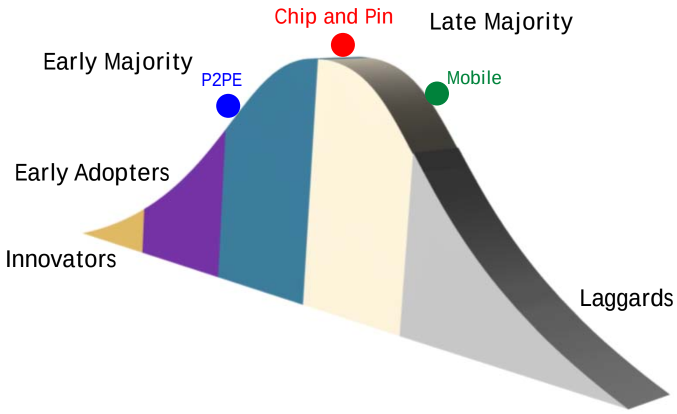
ACADEMIC IMPRESSIONS 4

POLL

Does your office use mobile payments? Chip & Pin?

PAYMENT ACCEPTANCE TRENDS IN ADVANCEMENT

TECHNOLOGY ADOPTION



So – What does this mean for PCI compliance?

WHAT ABOUT MOBILE PAYMENTS?

USING MOBILE

- Off campus fundraising events

PCI Compliant?

- “Other schools use it”
- “PCI Council addresses mobile”

MOBILE PAYMENTS?

CARD READERS: SMART PHONE/TABLETS

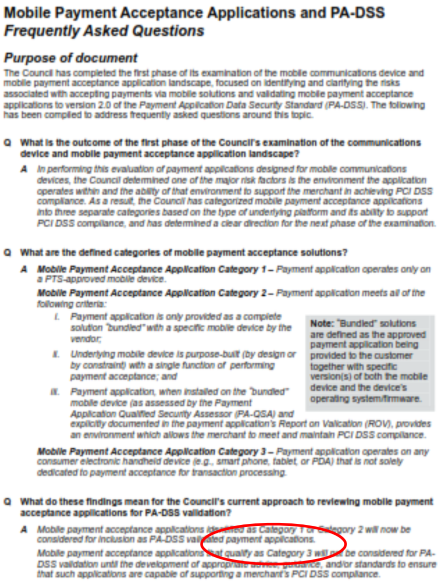
- “Square” and others
- “Category 3” device
- *None are certified compliant!*

MOBILE CARD TERMINALS

- Few are certified compliant
- Check with the PCI SSC

ACADEMIC IMPRESSIONS 9

MOBILE PAYMENTS?



Mobile Payment Acceptance Applications and PA-DSS
Frequently Asked Questions

Purpose of document

The Council has completed the first phase of its examination of the mobile communications device and mobile payment acceptance application landscape, focused on identifying and clarifying the risks associated with accepting payments via mobile solutions and validating mobile payment acceptance applications to version 2.0 of the *Payment Application Data Security Standard (PA-DSS)*. The following has been compiled to address frequently asked questions around this topic.

Q What is the outcome of the first phase of the Council's examination of the communications device and mobile payment acceptance application landscape?

A *In performing this evaluation of payment applications designed for mobile communications devices, the Council determined one of the major risk factors is the environment the application operates within and the ability of that environment to support the merchant in achieving PCI DSS compliance. As a result, the Council has categorized mobile payment acceptance applications into three separate categories based on the type of underlying platform and its ability to support PCI DSS compliance, and has determined a clear direction for the next phase of the examination.*

Q What are the defined categories of mobile payment acceptance solutions?

A ***Mobile Payment Acceptance Application Category 1 –*** *Payment application operates only on a PTS-approved mobile device.*

Mobile Payment Acceptance Application Category 2 – *Payment application meets all of the following criteria:*

i. Payment application is only provided as a complete solution "bundled" with a specific mobile device by the vendor;

ii. Underlying mobile device is purpose-built (by design or by constraint) with a single function of performing payment acceptance; and

iii. Payment application, when installed on the "bundled" mobile device (as assessed by the Payment Application Qualified Security Assessor (PA-QSA) and explicitly documented in the payment application's Report on Valication (ROV), provides an environment which allows the merchant to meet and maintain PCI DSS compliance.

Note: "Bundled" solutions are defined as the approved payment application being provided to the customer together with specific version(s) of both the mobile device and the device's operating system/firmware.

Mobile Payment Acceptance Application Category 3 – *Payment application operates on any consumer electronic handheld device (e.g., smart phone, tablet, or PDA) that is not solely dedicated to payment acceptance for transaction processing.*

Q What do these findings mean for the Council's current approach to reviewing mobile payment acceptance applications for PA-DSS validation?

A *Mobile payment acceptance applications identified as Category 1 or Category 2 will now be considered for inclusion as PA-DSS validated payment applications.*

Mobile payment acceptance applications that qualify as Category 3 will not be considered for PA-DSS validation until the development of appropriate advice, guidance, and/or standards to ensure that such applications are capable of supporting a merchant's PCI DSS compliance.

No Category 3 Device is considered compliant

ACADEMIC IMPRESSIONS 10

WHAT ABOUT CHIP AND PIN (EMV)?

WHAT IS THE PURPOSE?

- Prevents "cloning" a card
- Does NOT provide encryption
- Must be combined with P2PE for full encryption
- Does NOT address card-not-present transactions

EMV – European Mastercard/Visa
P2PE – Point-to-Point Encryption

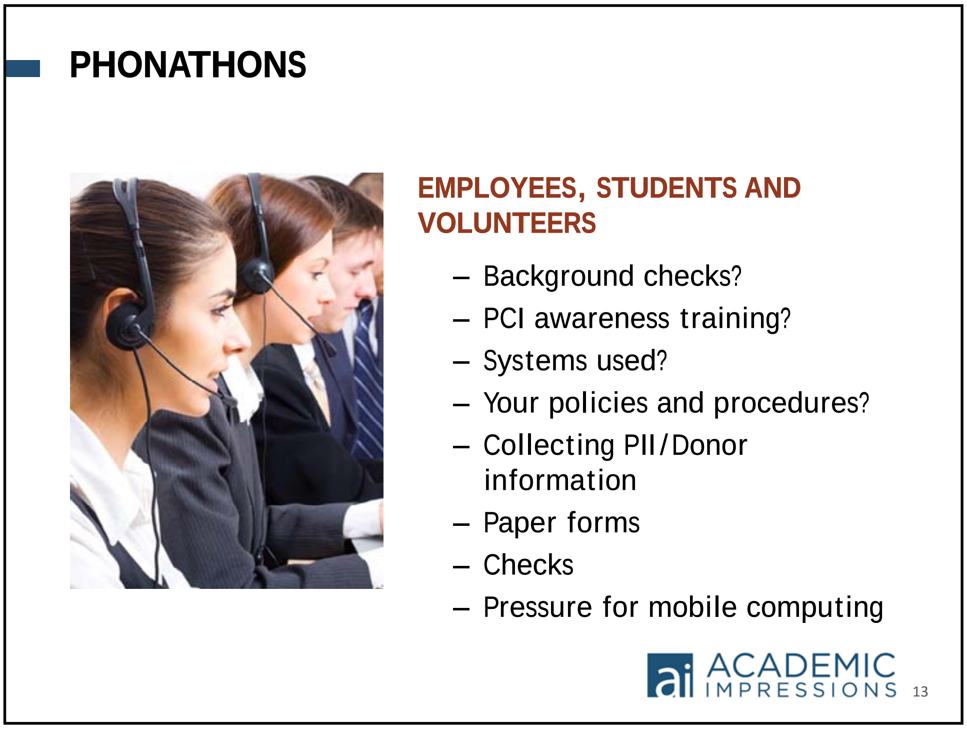
MOBILE PAYMENTS?

Bluefin Payment Systems

PayConex

Validated PCI Compliant

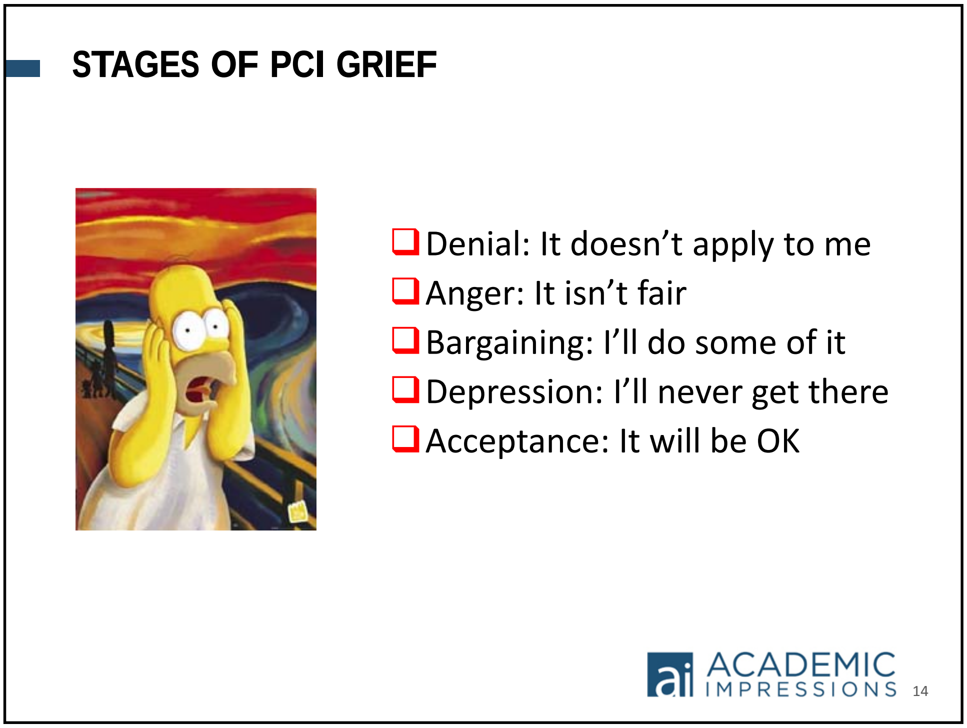
- P2PE



PHONATHONS

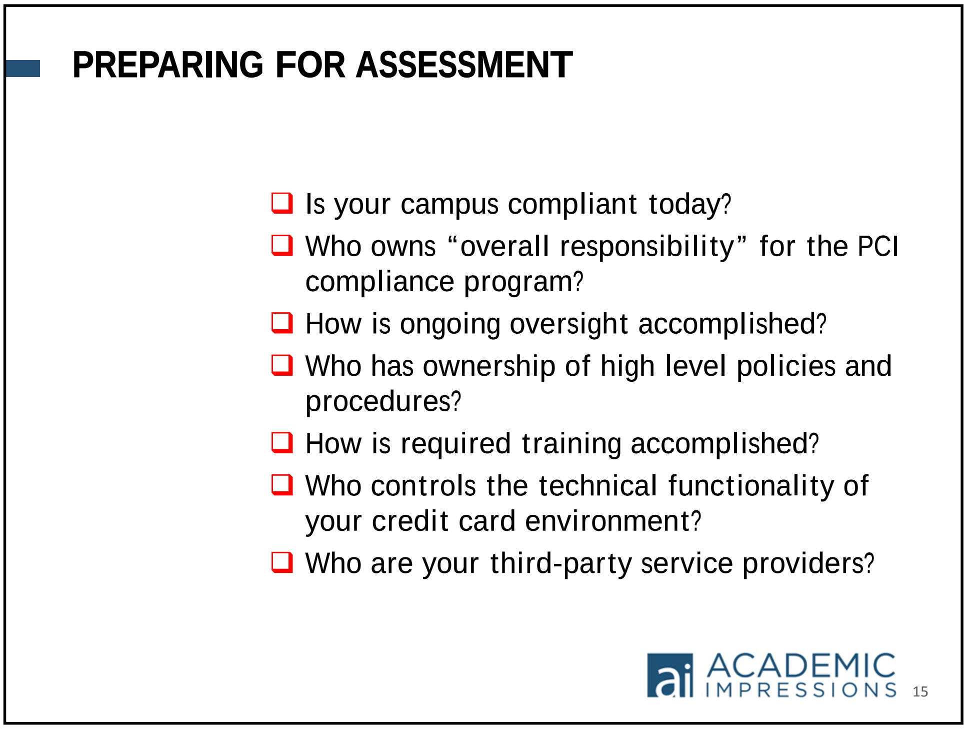
EMPLOYEES, STUDENTS AND VOLUNTEERS

- Background checks?
- PCI awareness training?
- Systems used?
- Your policies and procedures?
- Collecting PII/Donor information
- Paper forms
- Checks
- Pressure for mobile computing



STAGES OF PCI GRIEF

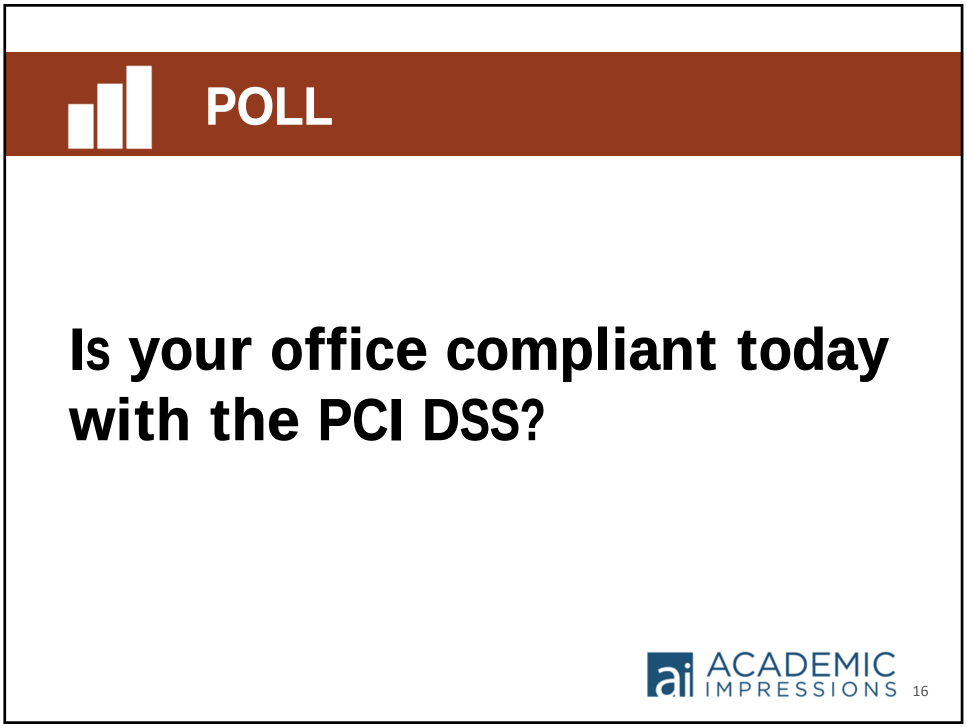
□ Denial: It doesn’t apply to me
□ Anger: It isn’t fair
□ Bargaining: I’ll do some of it
□ Depression: I’ll never get there
□ Acceptance: It will be OK



PREPARING FOR ASSESSMENT

- □ Is your campus compliant today?
- □ Who owns "overall responsibility" for the PCI compliance program?
- □ How is ongoing oversight accomplished?
- □ Who has ownership of high level policies and procedures?
- □ How is required training accomplished?
- □ Who controls the technical functionality of your credit card environment?
- □ Who are your third-party service providers?

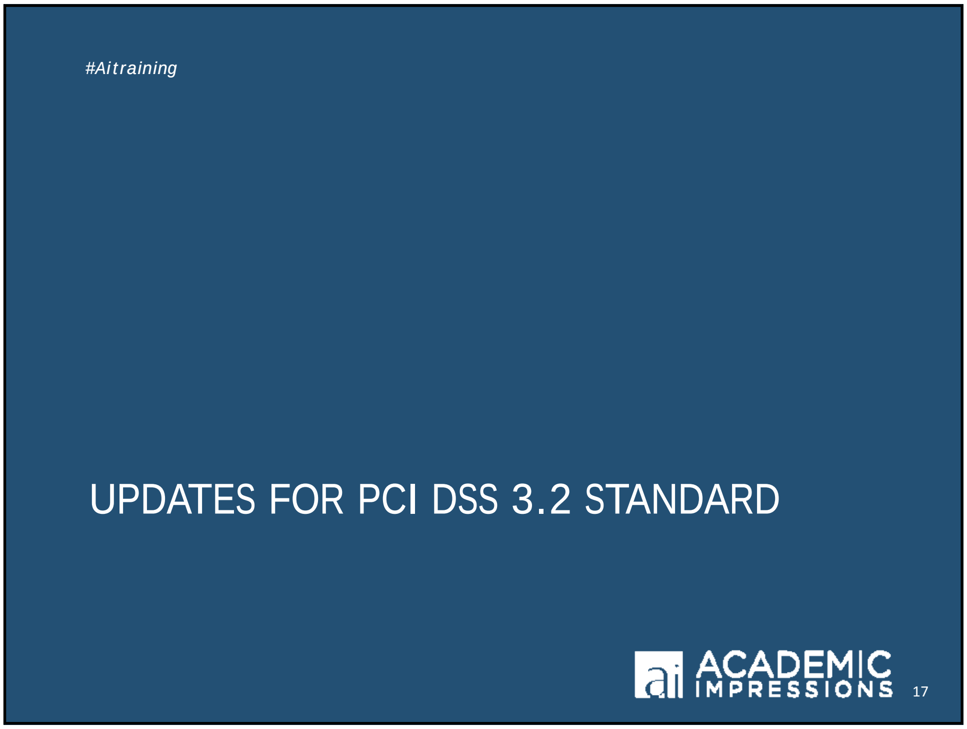
ACADEMIC IMPRESSIONS 15



POLL

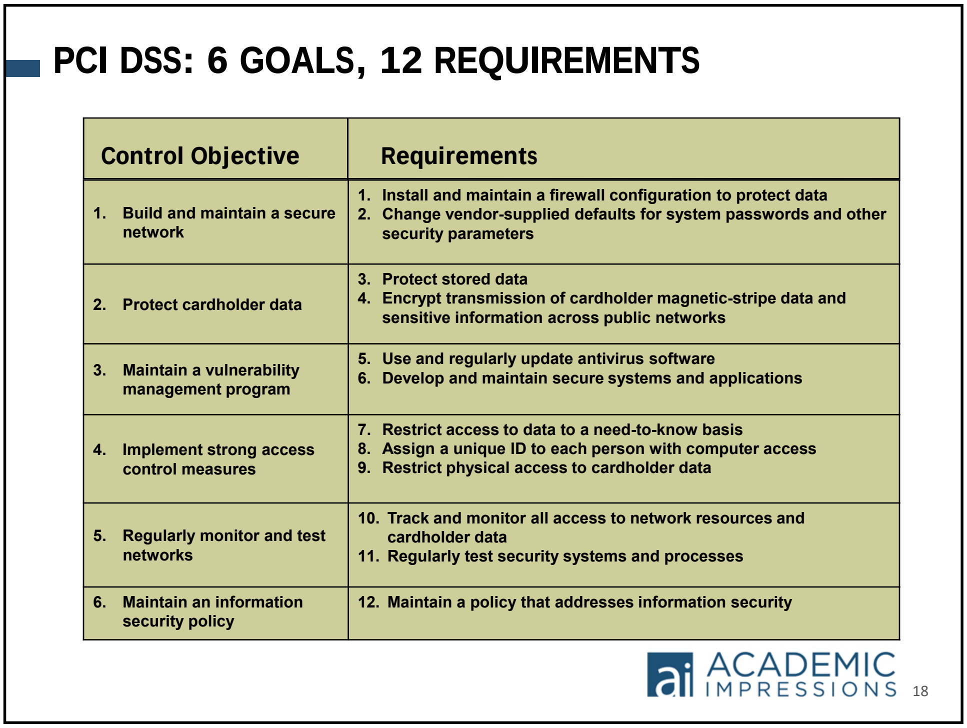
Is your office compliant today with the PCI DSS?

ACADEMIC IMPRESSIONS 16



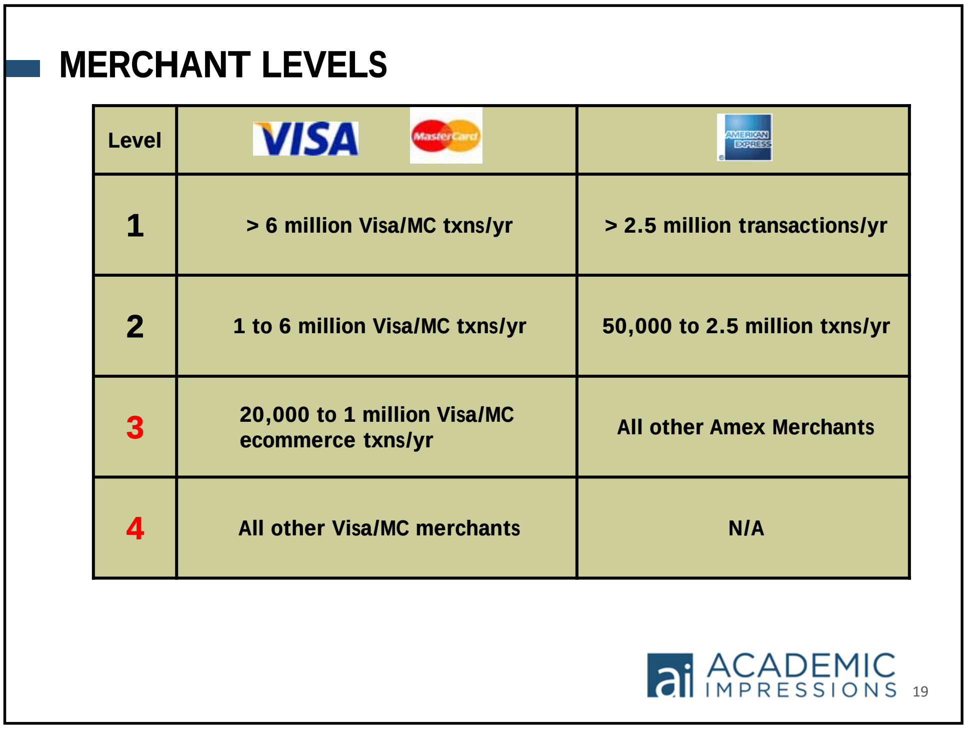
#Aitraining

UPDATES FOR PCI DSS 3.2 STANDARD



PCI DSS: 6 GOALS, 12 REQUIREMENTS

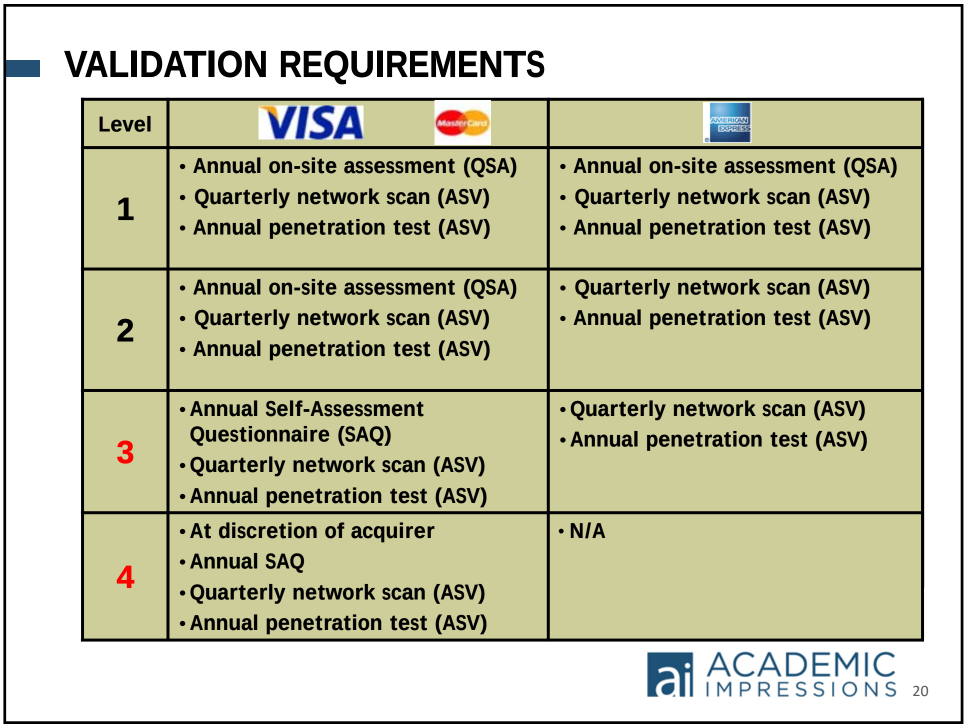
Control Objective	Requirements
1. Build and maintain a secure network	1. Install and maintain a firewall configuration to protect data 2. Change vendor-supplied defaults for system passwords and other security parameters
2. Protect cardholder data	3. Protect stored data 4. Encrypt transmission of cardholder 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

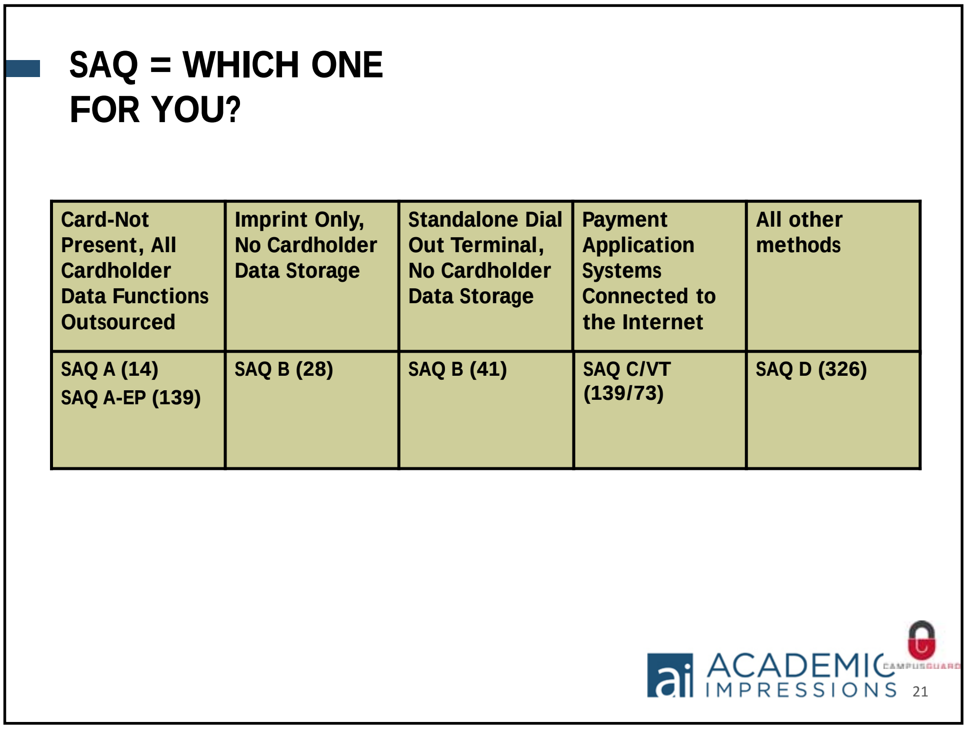
ai ACADEMIC IMPRESSIONS 19



VALIDATION REQUIREMENTS

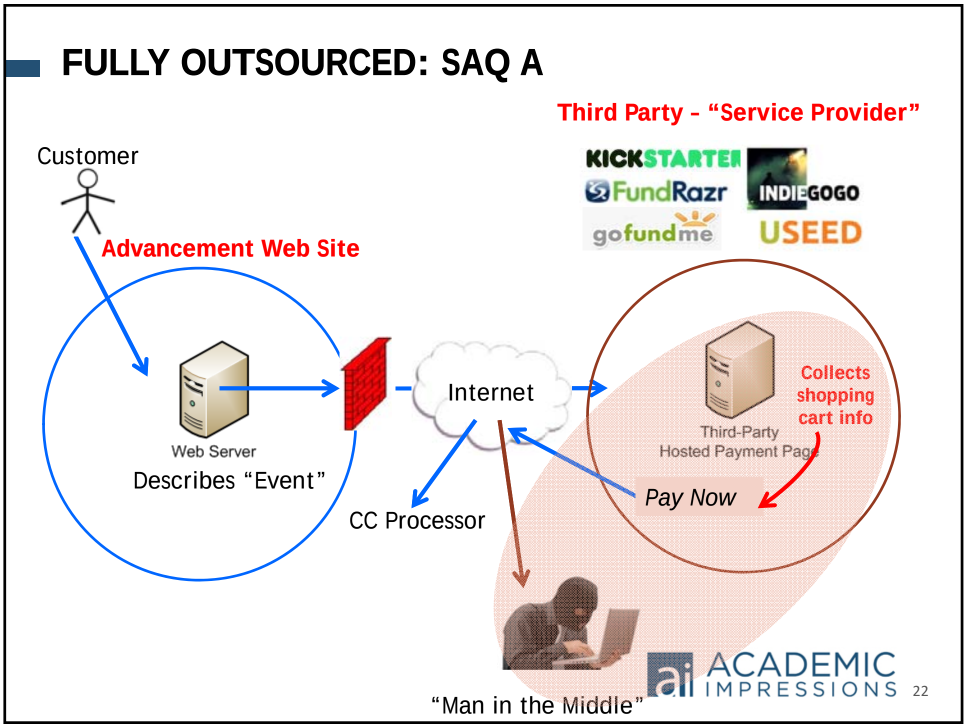
Level	VISA MasterCard	AMERICAN EXPRESS
1	• Annual on-site assessment (QSA) • Quarterly network scan (ASV) • Annual penetration test (ASV)	• Annual on-site assessment (QSA) • Quarterly network scan (ASV) • Annual penetration test (ASV)
2	• Annual on-site assessment (QSA) • Quarterly network scan (ASV) • 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

ai ACADEMIC IMPRESSIONS 20

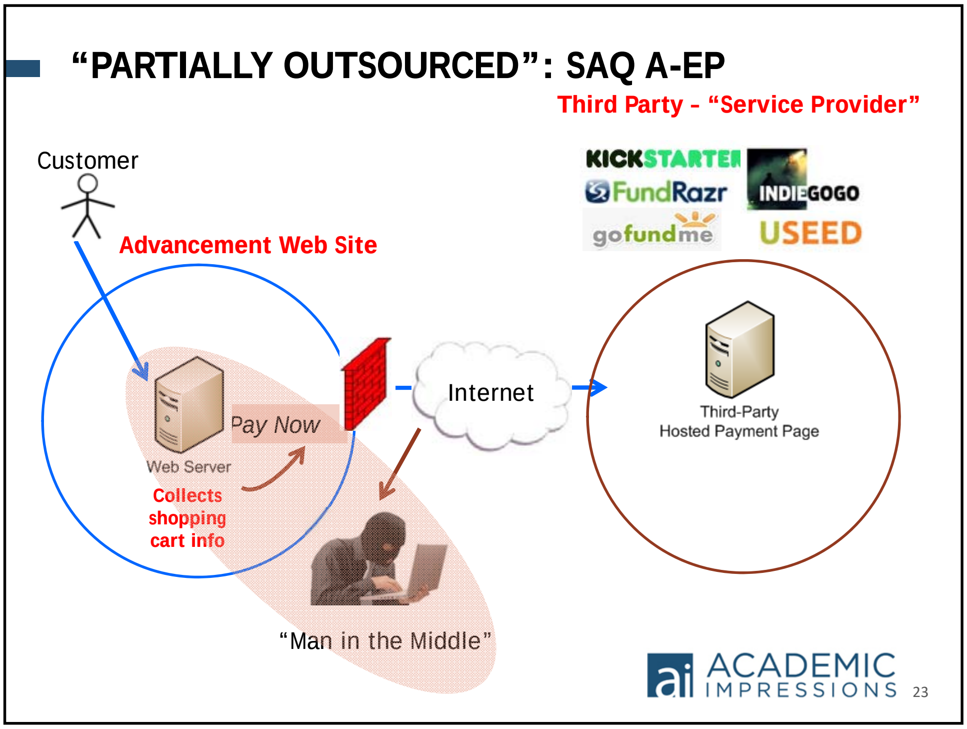


SAQ = WHICH ONE FOR YOU?

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 (14) SAQ A-EP (139)	SAQ B (28)	SAQ B (41)	SAQ C/VT (139/73)	SAQ D (326)



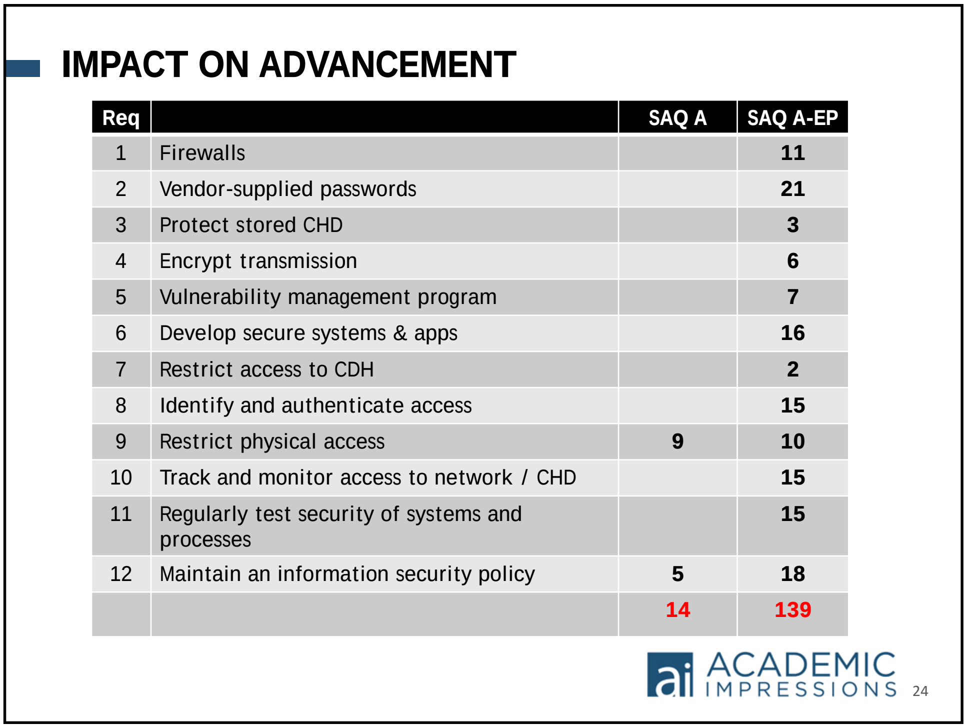
FULLY OUTSOURCED: SAQ A



"PARTIALLY OUTSOURCED": SAQ A-EP

Third Party - "Service Provider"

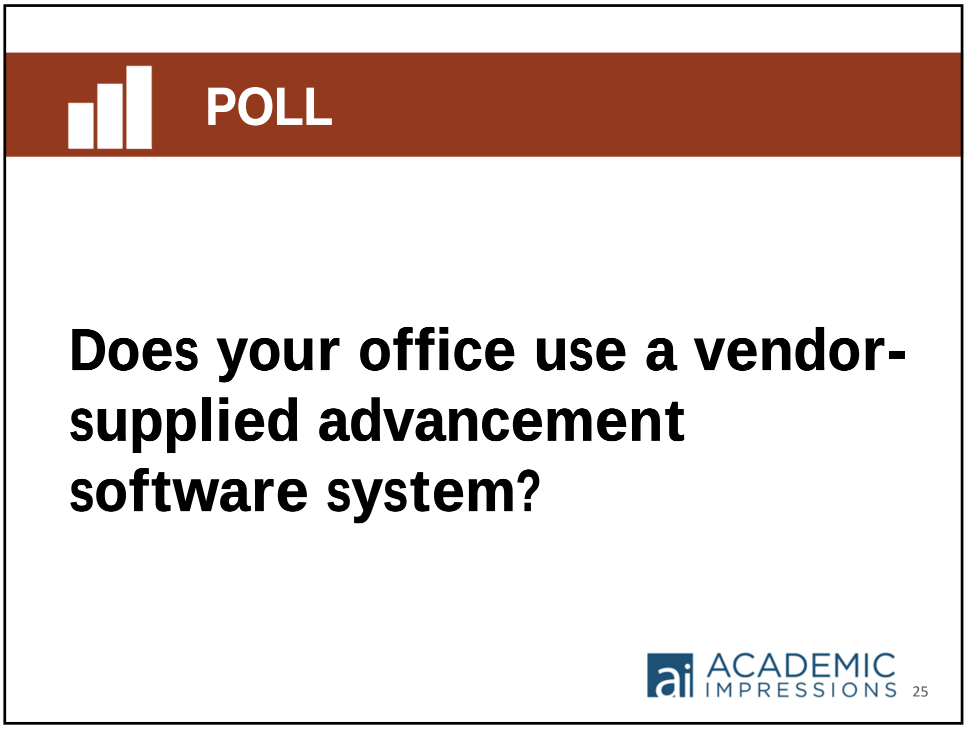
23



IMPACT ON ADVANCEMENT

Req		SAQ A	SAQ A-EP
1	Firewalls		**11**
2	Vendor-supplied passwords		**21**
3	Protect stored CHD		**3**
4	Encrypt transmission		**6**
5	Vulnerability management program		**7**
6	Develop secure systems & apps		**16**
7	Restrict access to CDH		**2**
8	Identify and authenticate access		**15**
9	Restrict physical access	**9**	**10**
10	Track and monitor access to network / CHD		**15**
11	Regularly test security of systems and processes		**15**
12	Maintain an information security policy	**5**	**18**
		14	**139**

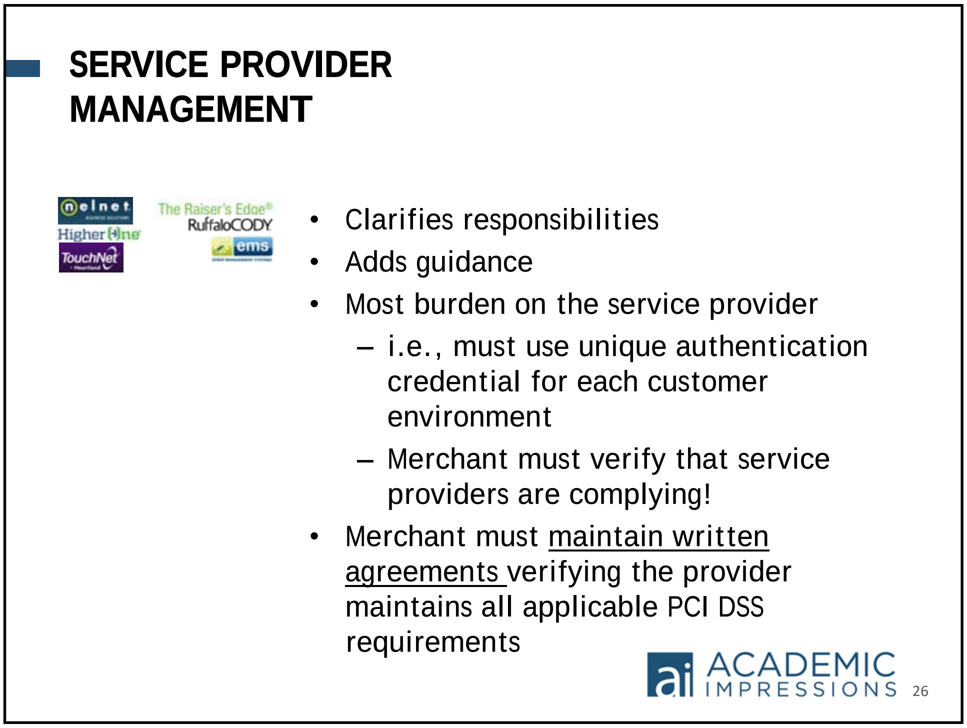
24



POLL

Does your office use a vendor-supplied advancement software system?

ACADEMIC IMPRESSIONS 25

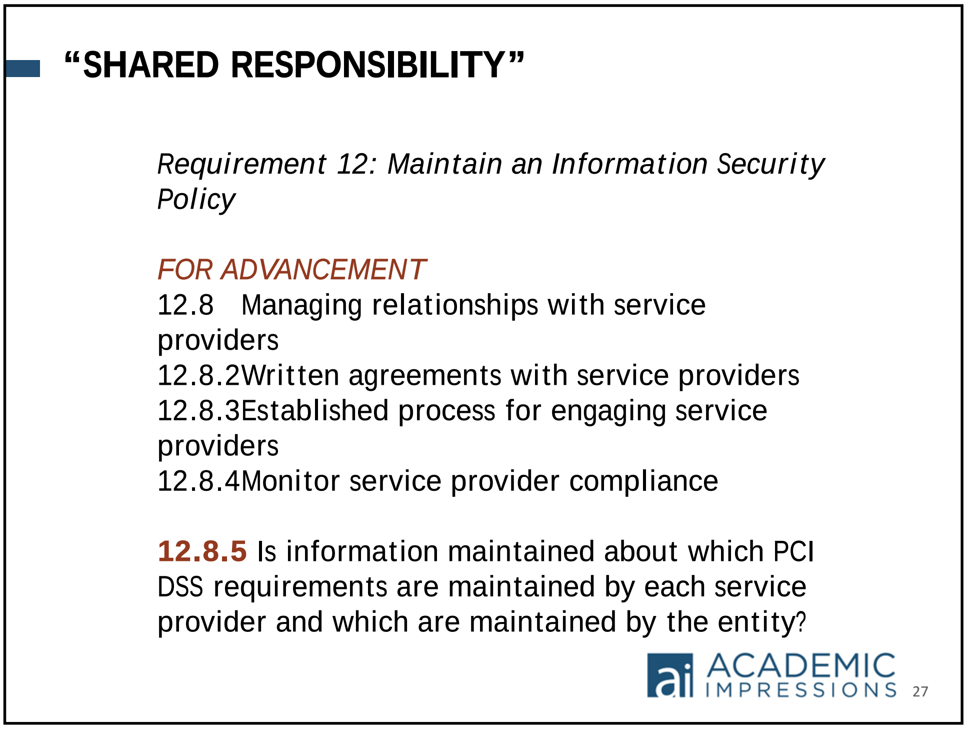


SERVICE PROVIDER MANAGEMENT

nelnet
Higher One
TouchNet
The Raiser's Edge
RuffaloCODY
ems

- Clarifies responsibilities
- Adds guidance
- Most burden on the service provider
  - i.e., must use unique authentication credential for each customer environment
  - Merchant must verify that service providers are complying!
- Merchant must maintain written agreements verifying the provider maintains all applicable PCI DSS requirements

ACADEMIC IMPRESSIONS 26



"SHARED RESPONSIBILITY"

Requirement 12: Maintain an Information Security Policy

FOR ADVANCEMENT

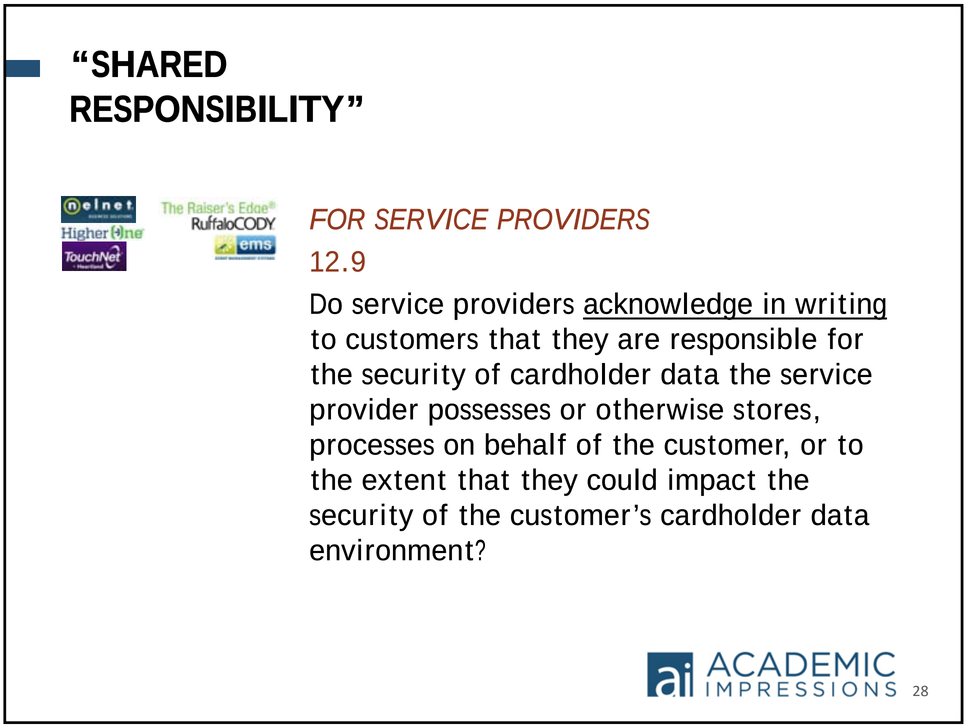
12.8 Managing relationships with service providers

12.8.2Written agreements with service providers

12.8.3Established process for engaging service providers

12.8.4Monitor service provider compliance

12.8.5 Is information maintained about which PCI DSS requirements are maintained by each service provider and which are maintained by the entity?

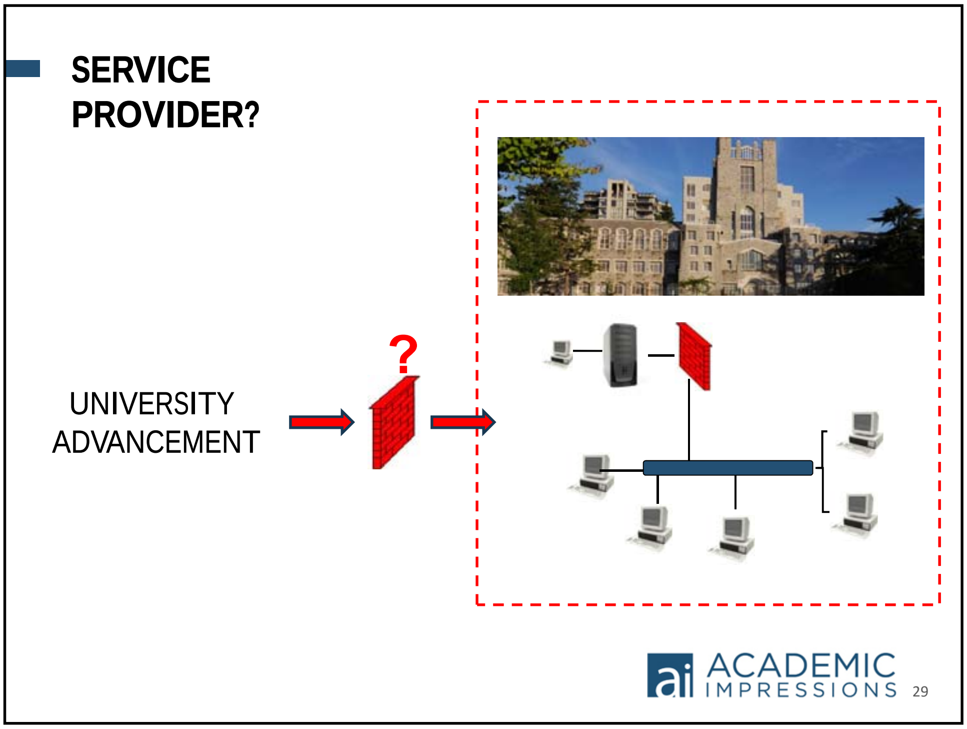


"SHARED RESPONSIBILITY"

FOR SERVICE PROVIDERS

12.9

Do service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?



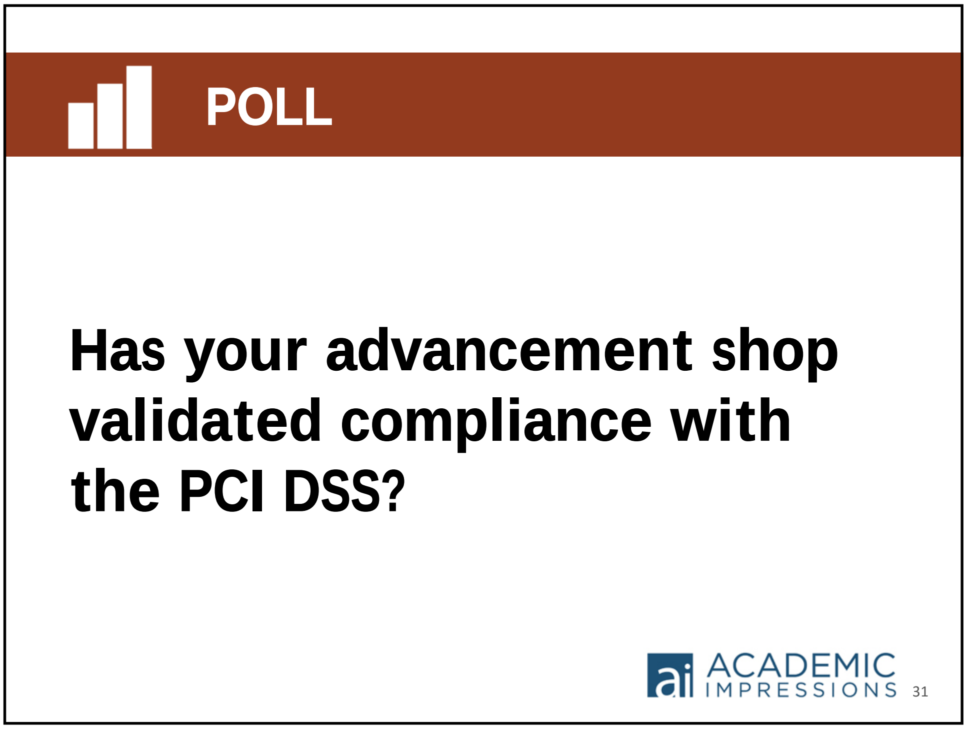
SERVICE PROVIDER?

ACADEMIC IMPRESSIONS 29

RESOURCE

Sample contract language

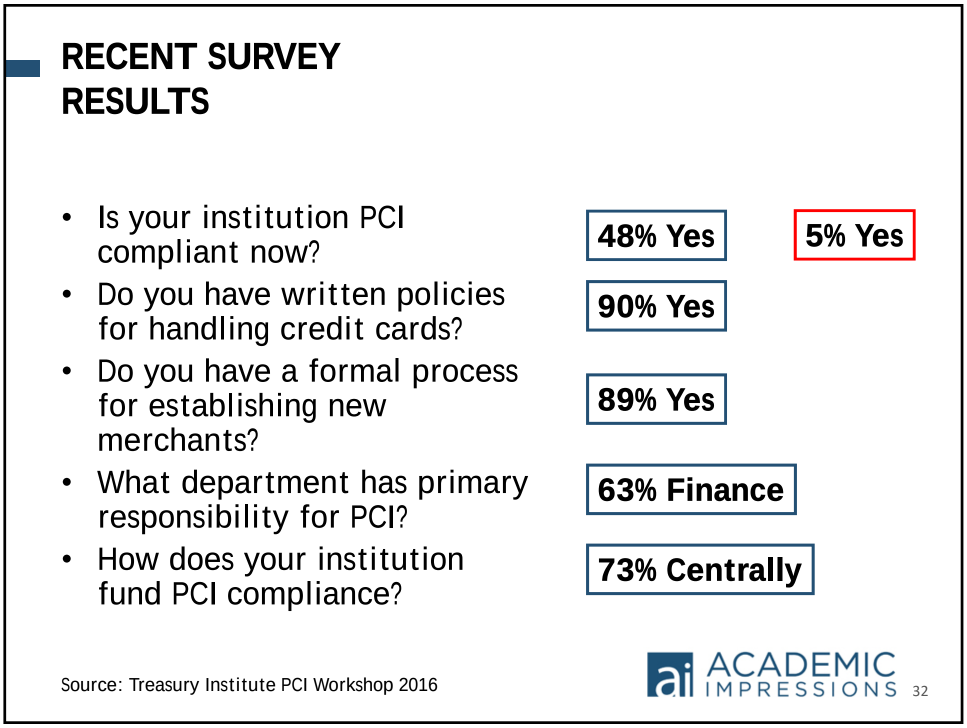
ACADEMIC IMPRESSIONS 30



POLL

Has your advancement shop validated compliance with the PCI DSS?

31



RECENT SURVEY RESULTS

Is your institution PCI compliant now?	**48% Yes**	**5% Yes**
Do you have written policies for handling credit cards?	**90% Yes**	
Do you have a formal process for establishing new merchants?	**89% Yes**	
What department has primary responsibility for PCI?	**63% Finance**	
How does your institution fund PCI compliance?	**73% Centrally**	

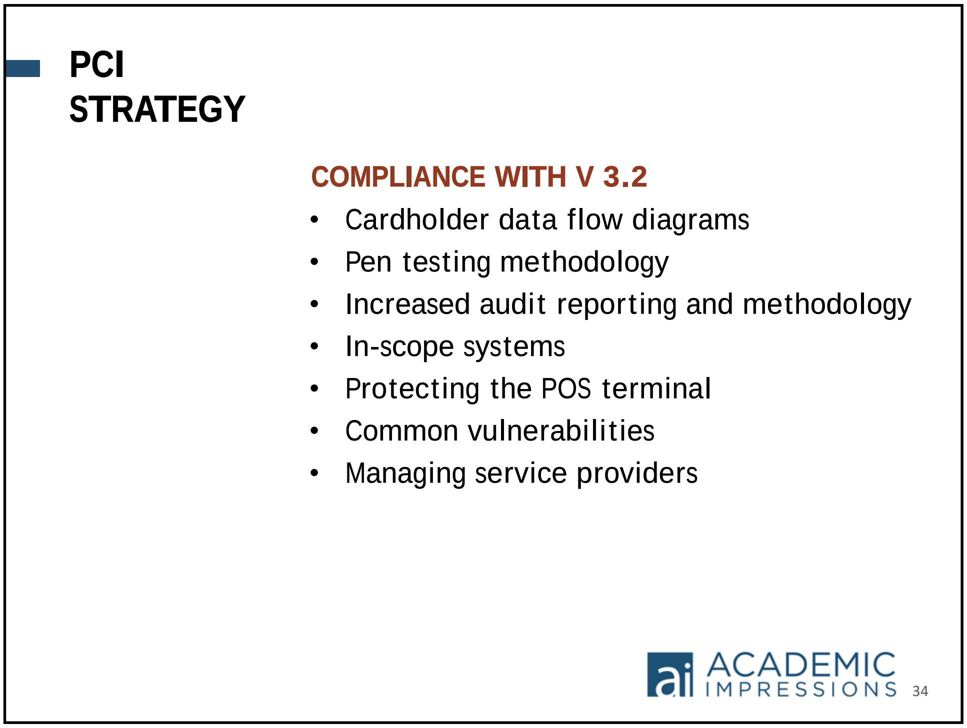
Source: Treasury Institute PCI Workshop 2016

32

#Aitraining

ENSURING COMPLIANCE

33



PCI STRATEGY

COMPLIANCE WITH V 3.2

- Cardholder data flow diagrams
- Pen testing methodology
- Increased audit reporting and methodology
- In-scope systems
- Protecting the POS terminal
- Common vulnerabilities
- Managing service providers

34

WHAT YOU SHOULD BE DOING NOW

- Review policies and procedures
- Review third-party contracts
- Review third-party software deployment
- Review relationship with the university
- Awareness training for all employees

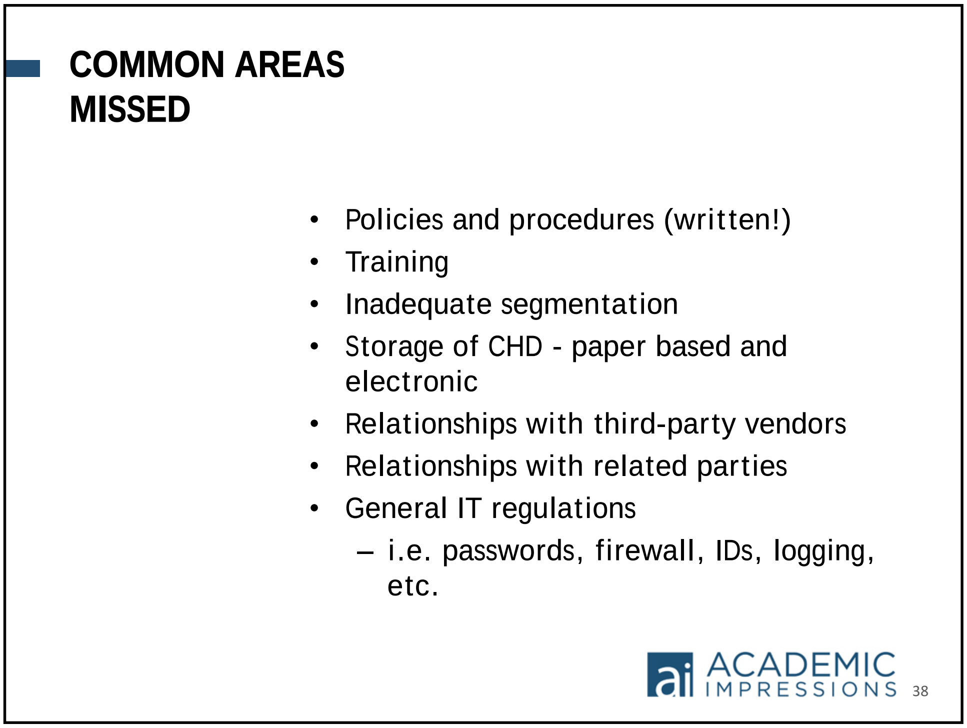
TRAINING?

- PCI Awareness
- Initial Employment
- Annual
- KEEP RECORDS!

#Aitraining

COMMON AREAS OF NON-COMPLIANCE

ACADEMIC IMPRESSIONS 37



COMMON AREAS MISSED

- Policies and procedures (written!)
- Training
- Inadequate segmentation
- Storage of CHD - paper based and electronic
- Relationships with third-party vendors
- Relationships with related parties
- General IT regulations
  - i.e. passwords, firewall, IDs, logging, etc.

ACADEMIC IMPRESSIONS 38

COMMON SENSE RULES "BUSINESS AS USUAL"

- Never leave a laptop or other computer device unattended
- Always log out of a computer when it is unattended
- Make sure anti-virus software is current and running
- Never download items without authorization
- If you suspect breach of security, contact IT department immediately

TAKEAWAYS

- Implement compliance as "business as usual"
- All employees, students, and volunteer workers are "in-scope"
- Awareness training a must!
- Involve your IT/network security department
- Make sure your business partners are PCI DSS compliant
- You are probably doing most things right already

RESOURCE

PCI
Now Available – PCI DSS 3.0
Welcome to the PCI Security Standards Council
MERCHANTS
FINANCIAL INSTITUTIONS
HARDWARE / SOFTWARE
SERVICES AND PROFESSIONALS

www.pcisecuritystandards.org

- SAQs
- FAQs
- White Papers
- Certified QSAs and ASVs

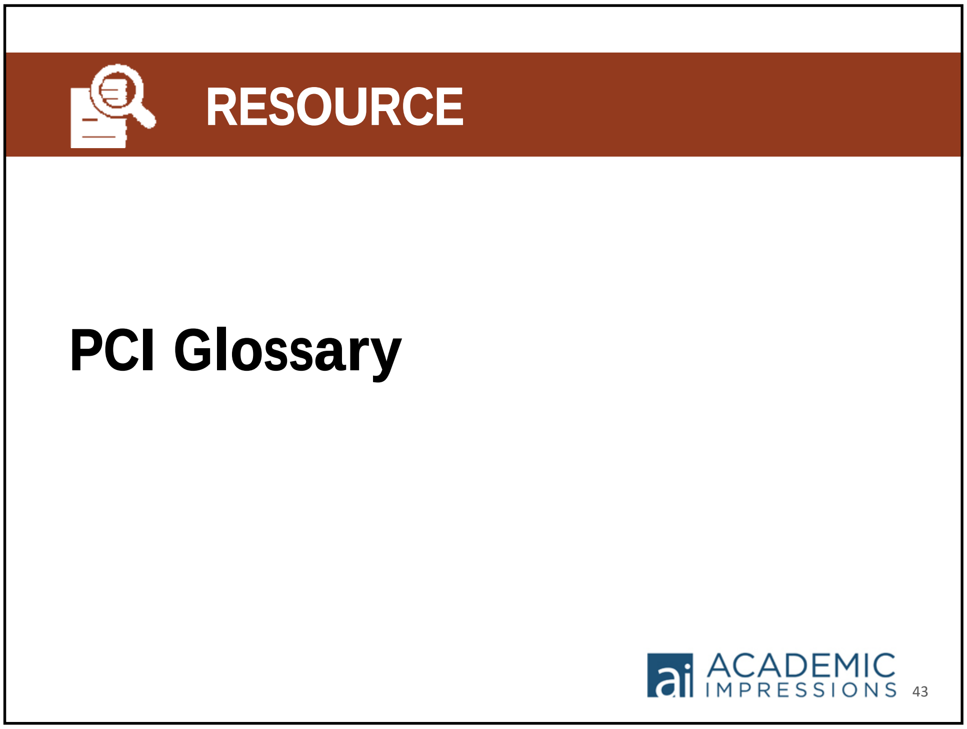
Treasury Institute
for Higher Education

www.treasuryinstitute.org

- Annual PCI Workshop
- Listserv
- Blog

RESOURCE

PCI Best Practices and Lessons Learned



RESOURCE

PCI Glossary

ACADEMIC IMPRESSIONS 43

RESOURCE

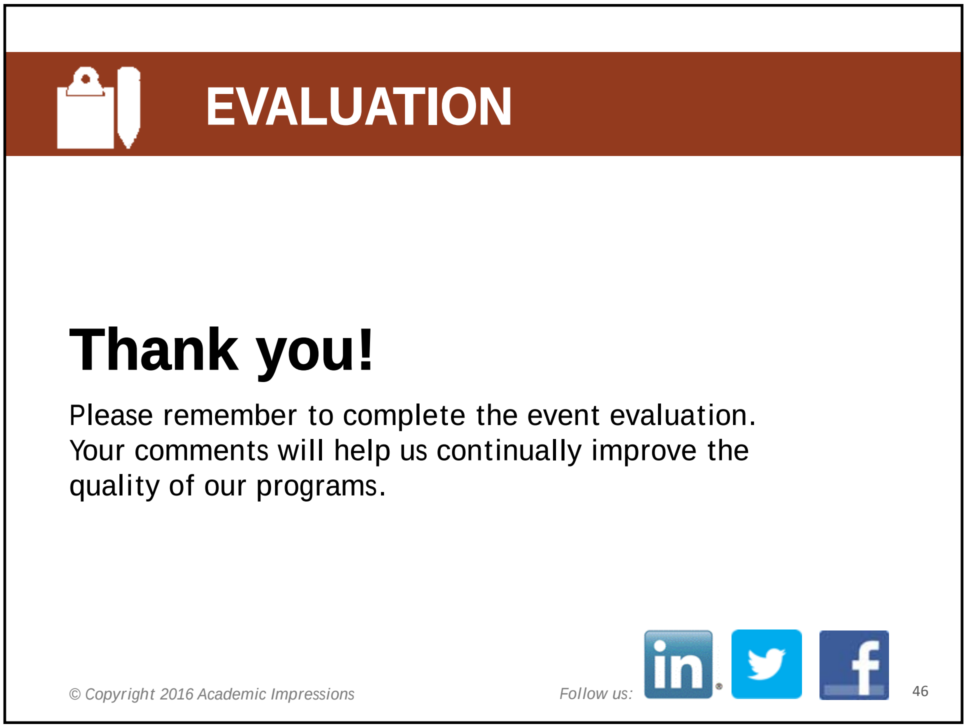
Sample Policies and Procedures

ACADEMIC IMPRESSIONS 44

QUESTIONS

Ron King | rking@campusguard.com | 972-964-8884

45



EVALUATION

Thank you!

Please remember to complete the event evaluation. Your comments will help us continually improve the quality of our programs.

Follow us:

46