# GET THE PCI DSS COMPLIANCE PROGRAM YOU NEED

**Carolann G Lazarus, CISA, CCEP**
**IT Audit Manager**
**State University of New York, University at Buffalo**
**PCI Compliance Initiative Co-Lead**

**Higher Education Compliance Conference - SCCE**
**Tuesday June 11, 2019**

**Internal Audit**

1

**University at Buffalo** The State University of New York

- ❑ UB is a research-intensive public university founded in 1846.
- ❑ We are the largest and most comprehensive campus in the 64-campus SUNY system.
- ❑ We have three campuses that encompass nearly 1,250 acres and 200 buildings.
- ❑ We offer over 125 undergraduate degrees and over 320 graduate, professional and certificate programs.
- ❑ Our student body consists of over 21,000 undergraduates and almost 10,000 graduate and professional students.
- ❑ We employee just over 6,000 full-time equivalent employees.

2

# Agenda

- All about me
- PCI DSS Overview
- Recognition
- Key Components
- Hurdles & Solutions
- Tools & Resources
- Questions
- Bonus

# ABOUT ME

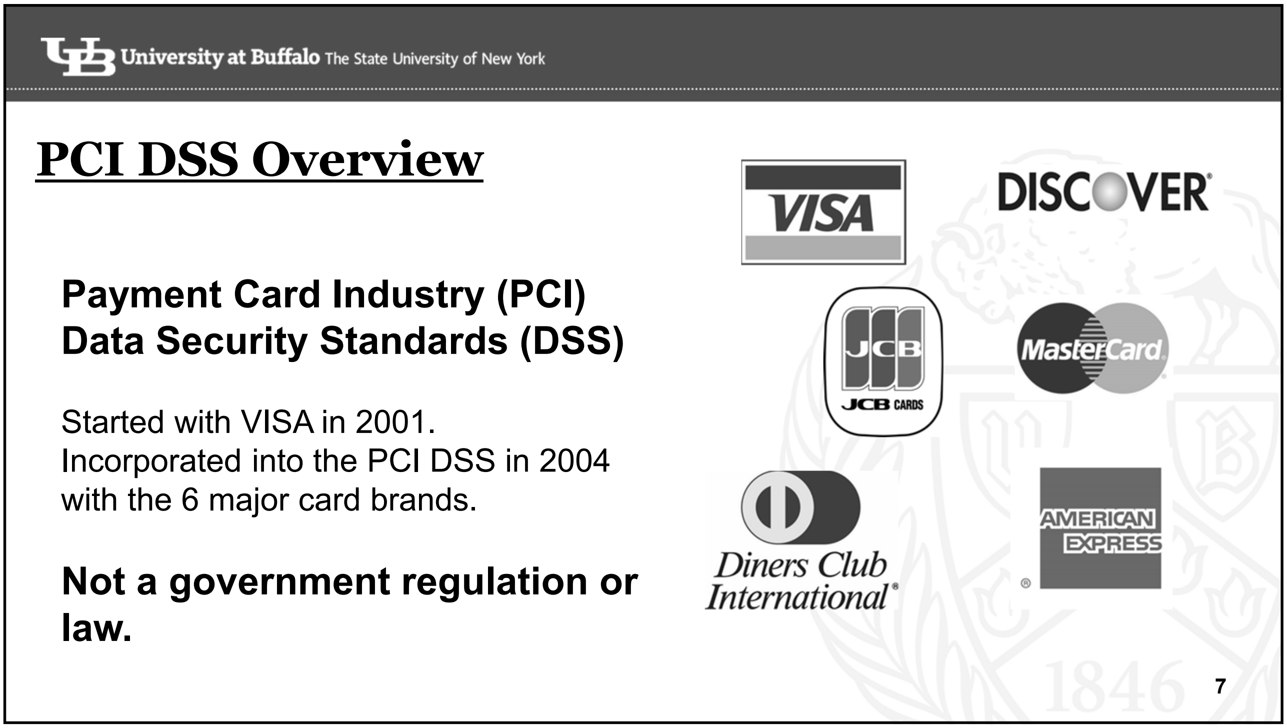
- Co-Lead of the PCI Compliance Initiative, which has recently morphed into the PCI Compliance Committee
- Significant audit experience with compliance in higher education
- CCEP

Our PCI Compliance Initiative

"This is a major project of utmost importance, but it has no budget, no guidelines, no support staff, and it's due in 15 minutes. At last, here's your chance to really impress everyone!"

# PCI DSS OVERVIEW

Payment Card Industry Data Security Standard



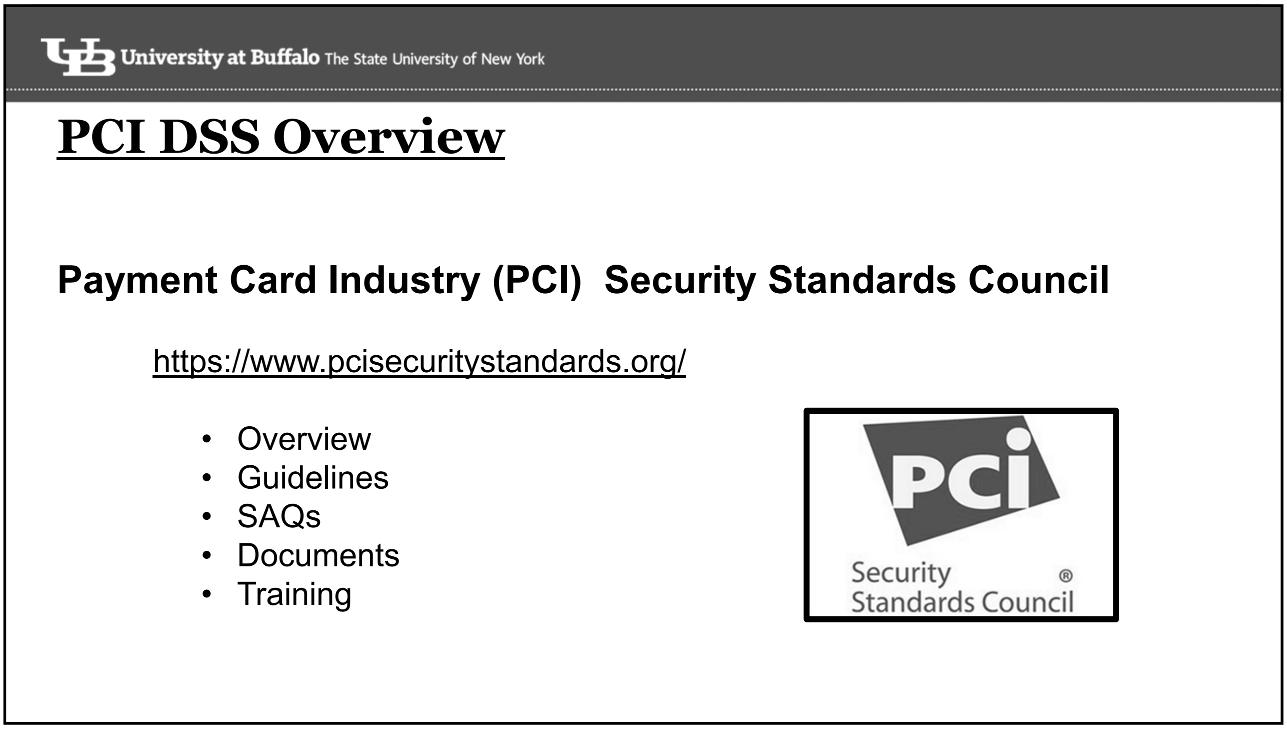
## PCI DSS Overview

**Payment Card Industry (PCI) Data Security Standards (DSS)**

Started with VISA in 2001.
Incorporated into the PCI DSS in 2004 with the 6 major card brands.

**Not a government regulation or law.**

VISA
DISCOVER
JCB
JCB CARDS
MasterCard
Diners Club International
AMERICAN EXPRESS
1846



## PCI DSS Overview

**Payment Card Industry (PCI) Security Standards Council**

https://www.pcisecuritystandards.org/

- Overview
- Guidelines
- SAQs
- Documents
- Training

PCi
Security Standards Council ®

University at Buffalo The State University of New York

# PCI DSS Overview

Developed to increase control of card holder data in order to reduce credit card fraud and exposure

Applies to all merchants and service providers that store, process or transmit cardholder account data, regardless of volume

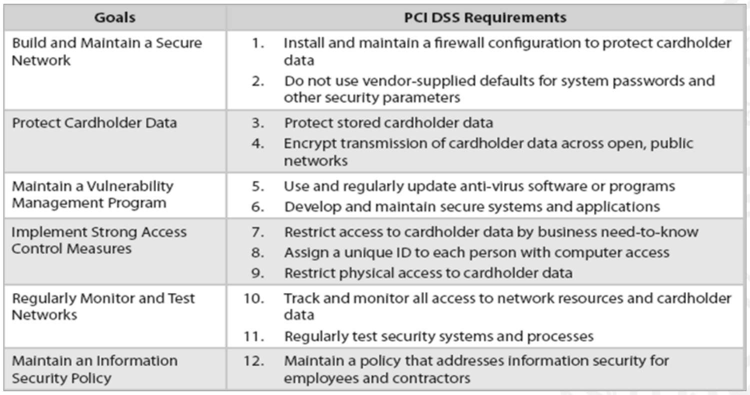
Updated annually, major update every three years – last major in April 2016

All merchants must annually self-assess compliance – SAQ’s

Consequences include fines, penalties and ineligibility to process credit cards in addition to brand and reputation damage

University at Buffalo The State University of New York

## 6 Goals and 12 Requirements of the PCI DSS



| Goals | PCI DSS Requirements |
|---|---|
| Build and Maintain a Secure Network | 1. Install and maintain a firewall configuration to protect cardholder data<br>2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data | 3. Protect stored cardholder data<br>4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | 5. Use and regularly update anti-virus software or programs<br>6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 7. Restrict access to cardholder data by business need-to-know<br>8. Assign a unique ID to each person with computer access<br>9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data<br>11. Regularly test security systems and processes |
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security for employees and contractors |

Depending on the method used to accept credit card payments, some of these requirements may not be applicable. For example, only a few apply to a department that uses a credit card terminal connected to an analog or cellular phone line to process credit card payments.

# Why Do We Need a PCI Compliance Program?

WHY?

- ❖ Protect the institutions customers. Students, Parents, Faculty, Staff

WHY?

- ❖ Protect the institutions reputation and resources
- ❖ Reduce risk of penalties

***University of Connecticut Hack Exposed Students' Credit Cards, SSNs***

CYBERATTACK 101: WHY HACKERS ARE GOING AFTER UNIVERSITIES

***"Data Breaches Put a Dent in Colleges' Finances as Well as Reputations"***

**The costs of a breach can run into the millions of dollars, according to data-security professionals who work in higher education.**

**$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $**

# RECOGNITION

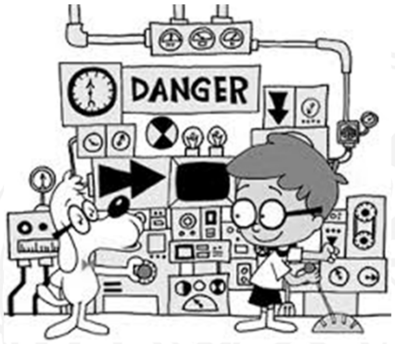
How do you know your program needs improvement?

13

## Recognizing the Need

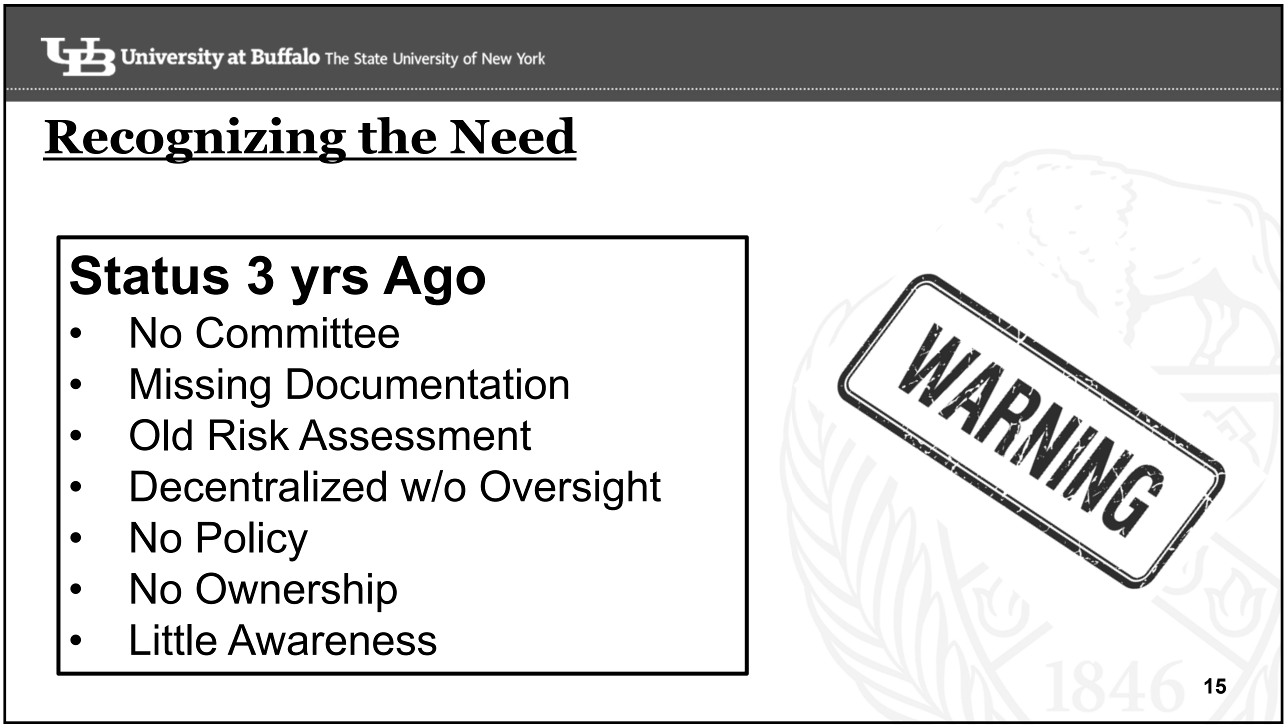
### Historic Actions 10+ yrs

- Committee
- Define category and level
- Identify merchants
- IT Networks
- Scanning
- SAQs
- Policies and Procedures



Wayback Machine

14

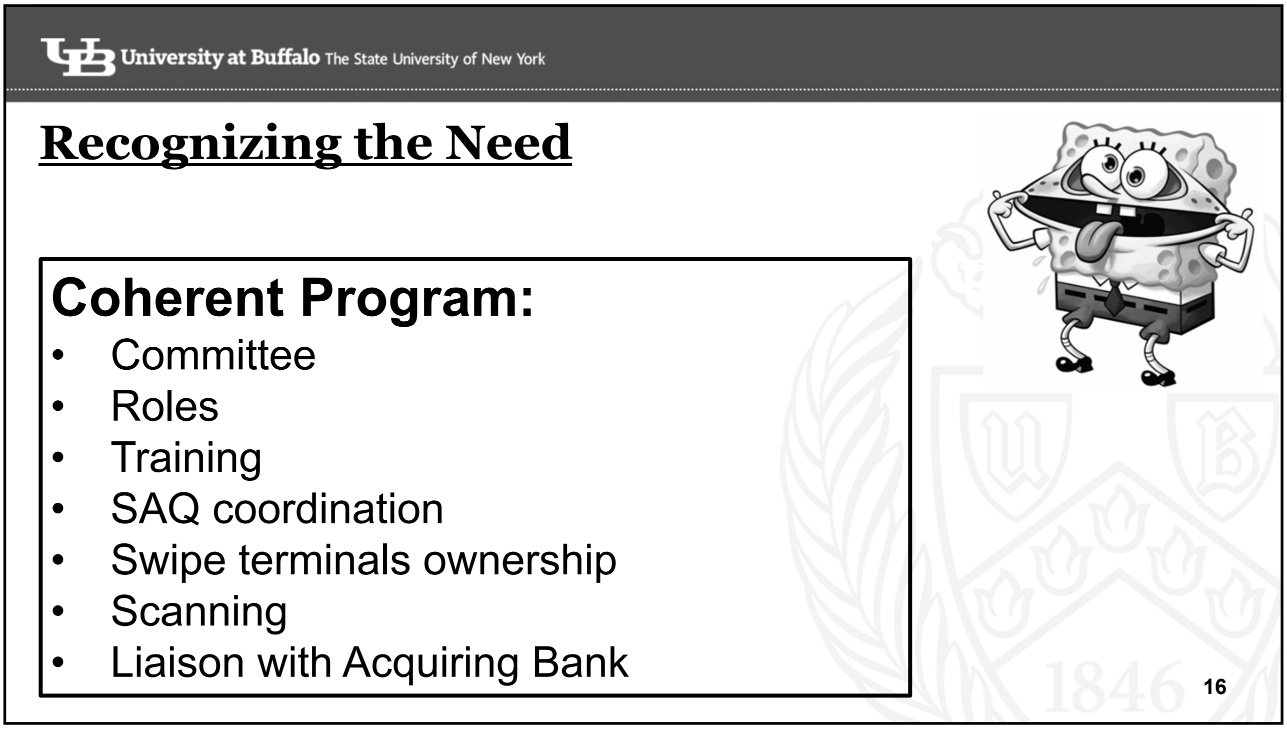


## Recognizing the Need

**Status 3 yrs Ago**

- No Committee
- Missing Documentation
- Old Risk Assessment
- Decentralized w/o Oversight
- No Policy
- No Ownership
- Little Awareness

15

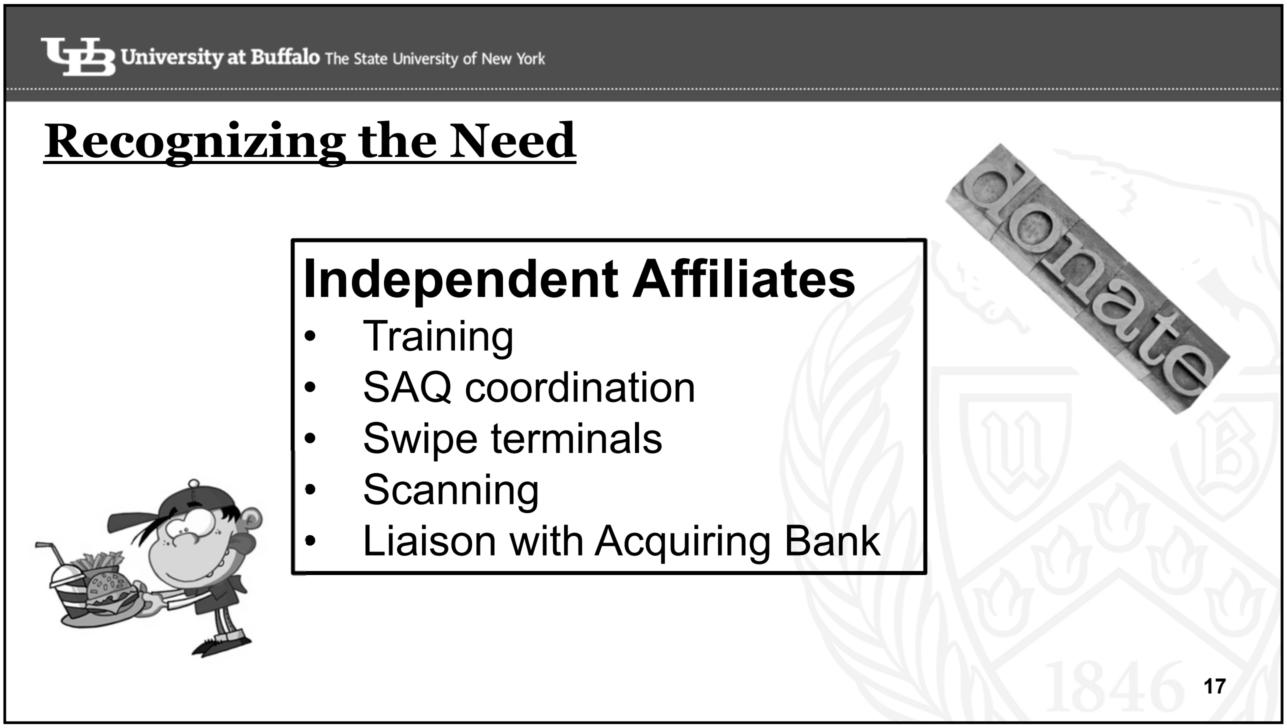


## Recognizing the Need

**Coherent Program:**

- Committee
- Roles
- Training
- SAQ coordination
- Swipe terminals ownership
- Scanning
- Liaison with Acquiring Bank

16



University at Buffalo The State University of New York

## Recognizing the Need

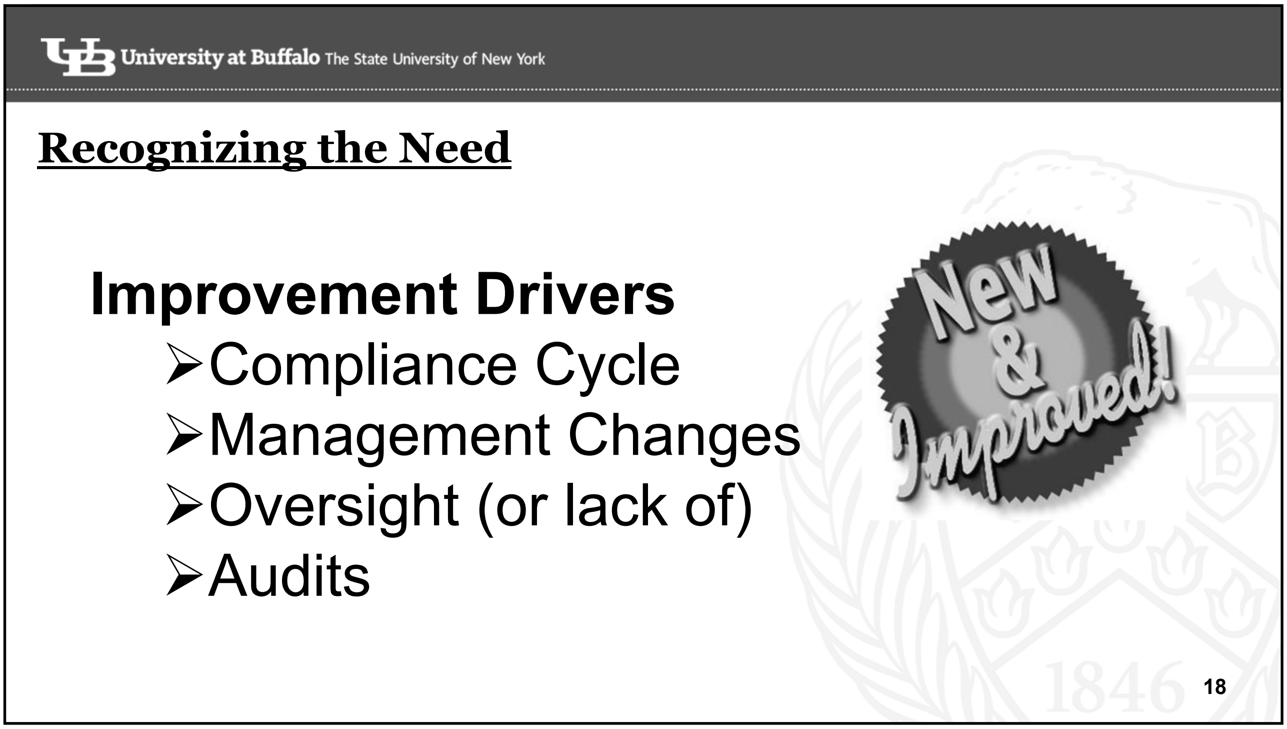
**Independent Affiliates**

- Training
- SAQ coordination
- Swipe terminals
- Scanning
- Liaison with Acquiring Bank

donate
1846

17

17



University at Buffalo The State University of New York

## Recognizing the Need

**Improvement Drivers**

- ➢Compliance Cycle
- ➢Management Changes
- ➢Oversight (or lack of)
- ➢Audits

New
&
Improved!
1846

18

18

University at Buffalo The State University of New York

# KEY COMPONENTS

- Can you Pass an Audit?
- What Don't you Know?
- PCI Committee

19

University at Buffalo The State University of New York

## Key Components

### Can you pass an audit?

- Risk Assessment
- Defined Roles
- SAQ's
- Policy & Procedures
- Training
- IT Security
- Data Flow Diagram

20

## Key Components

**What Don’t You Know?**

- What’s your transaction level
- How many merchants do you have?
- How much do you process $$?
- Who’s your acquiring bank?
- Which SAQ(s) do you need to complete?
- How many staff require training and what percentage have?
- Are your policy and procedures up-to-date?
- Who’s your QSA?

## Key Components

**PCI Committee**

- Standing
- Representative
- Accountable
- Acts as a Steering Committee
- Takes Action
- Performs Oversight
- Compliance Program

University at Buffalo The State University of New York

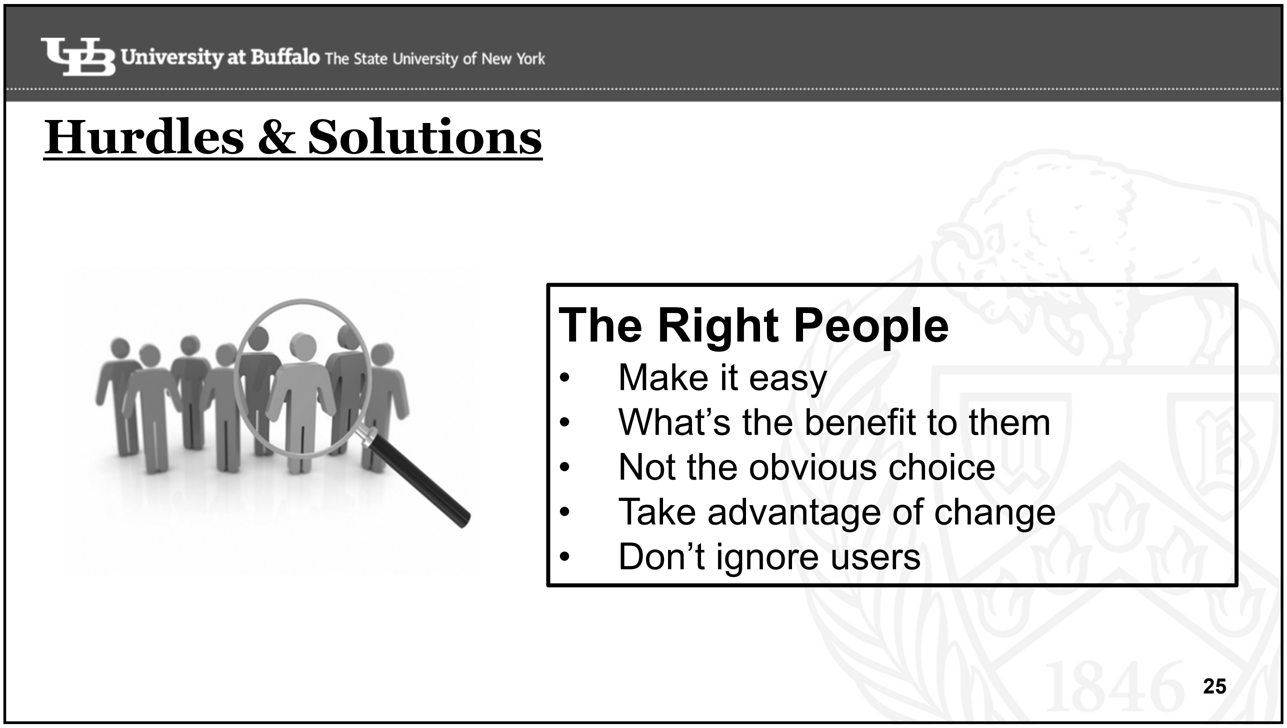
# HURDLES & SOLUTIONS

University at Buffalo The State University of New York

## Hurdles & Solutions

**The Wrong People**

- Sponsors
- Committee Members
- Subject Matter Experts



University at Buffalo The State University of New York

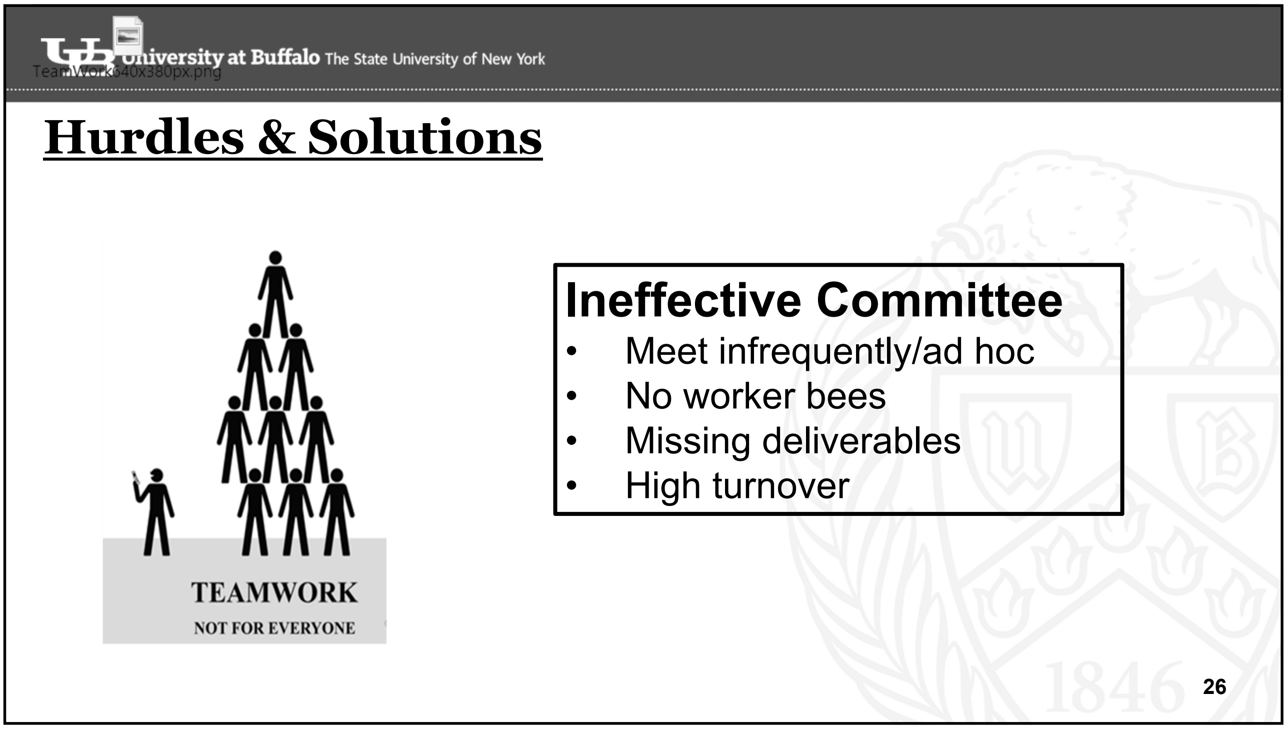
## Hurdles & Solutions

### The Right People

- Make it easy
- What's the benefit to them
- Not the obvious choice
- Take advantage of change
- Don't ignore users

25

25



University at Buffalo The State University of New York

TeamWork640x380px.png

## Hurdles & Solutions

### Ineffective Committee

- Meet infrequently/ad hoc
- No worker bees
- Missing deliverables
- High turnover

26

26

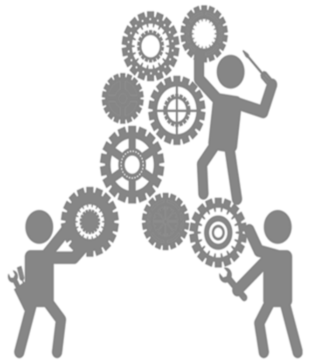
University at Buffalo The State University of New York

TeamWork640x380px.png

# Hurdles & Solutions

## Functional Committee

- Ownership / Leadership
- Rules
- Training
- Planned turnover
- Scheduled, sufficient meetings
- Accountability
- Valued



1846

27

27

University at Buffalo The State University of New York

TeamWork640x380px.png

# Hurdles & Solutions

## Lack of Knowledge

- Ultimate arbiter
- Awareness
- Direction

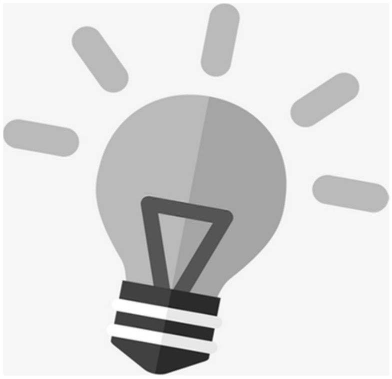
1846

28

28

TeamWork640x380px.png

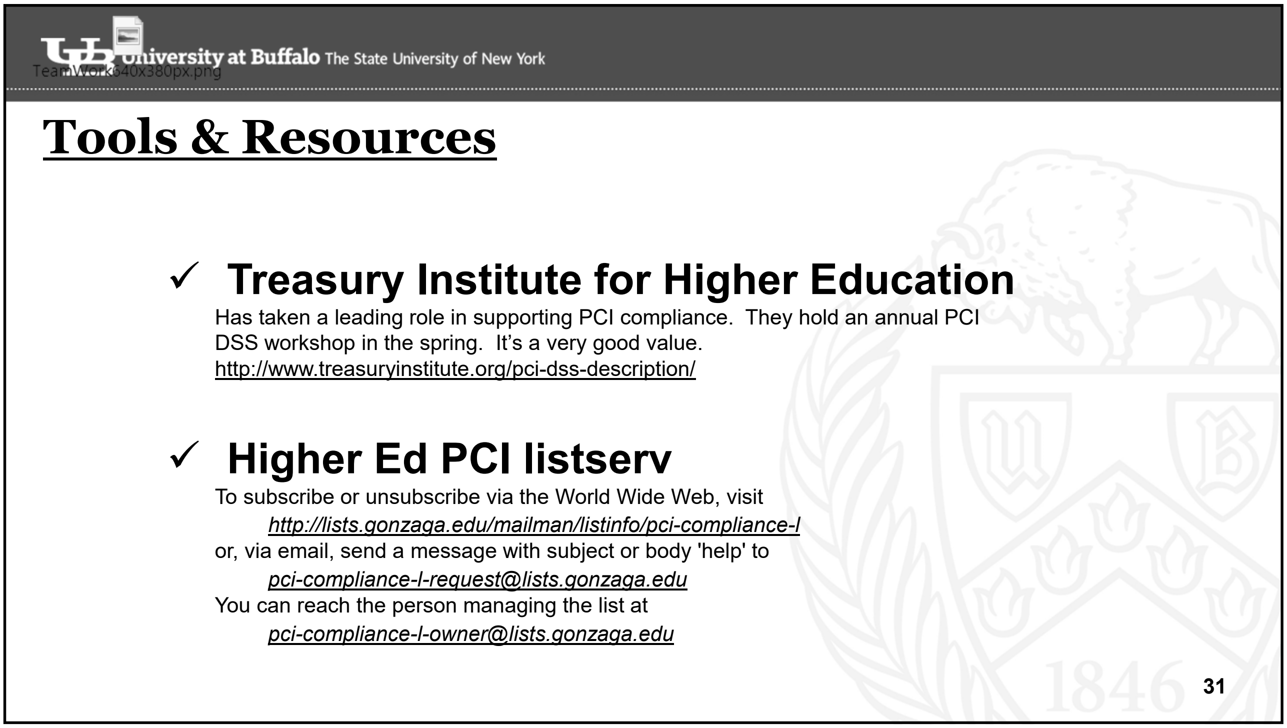
## Hurdles & Solutions



**Understanding**

- QSA
- Training
- Awareness Activities
- Surveys
- Documentation

# TOOLS & RESOURCES



University at Buffalo The State University of New York

TeamWork640x380px.png

## Tools & Resources

- ✓ **Treasury Institute for Higher Education**

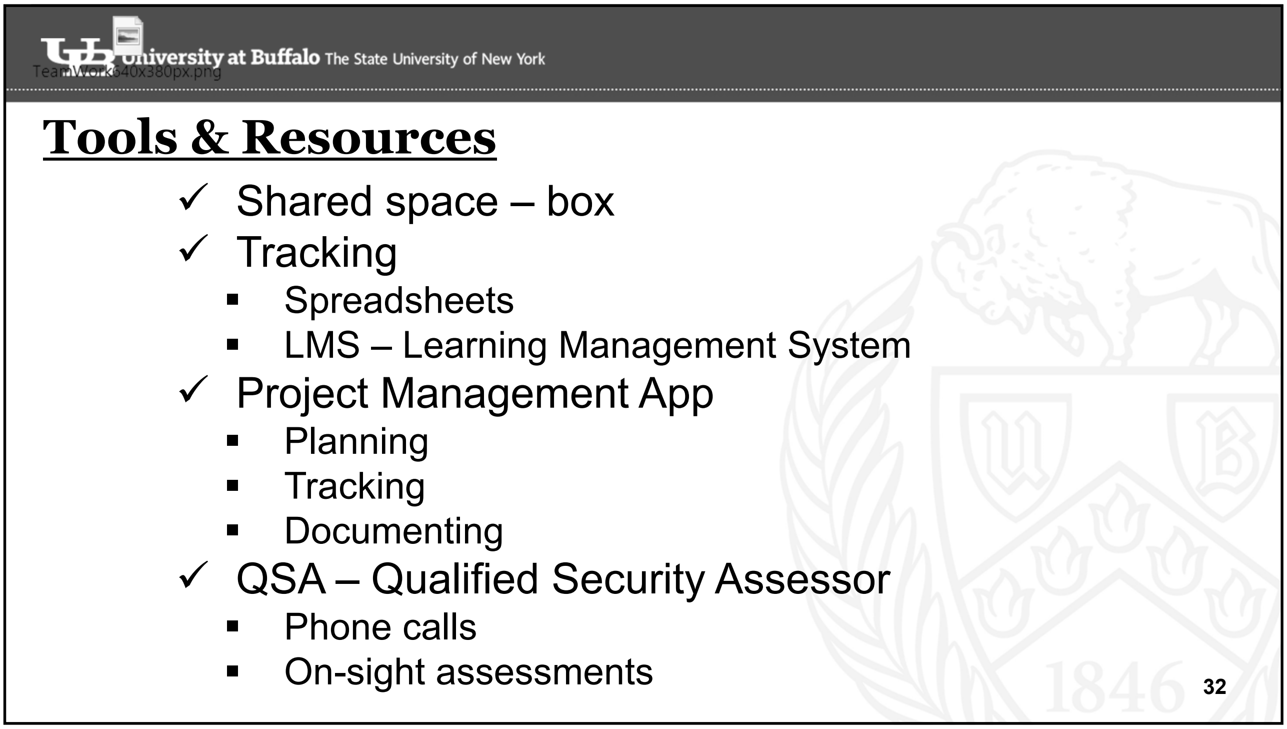
  Has taken a leading role in supporting PCI compliance. They hold an annual PCI DSS workshop in the spring. It's a very good value.
  http://www.treasuryinstitute.org/pci-dss-description/

- ✓ **Higher Ed PCI listserv**

  To subscribe or unsubscribe via the World Wide Web, visit
  *http://lists.gonzaga.edu/mailman/listinfo/pci-compliance-l*
  or, via email, send a message with subject or body 'help' to
  *pci-compliance-l-request@lists.gonzaga.edu*
  You can reach the person managing the list at
  *pci-compliance-l-owner@lists.gonzaga.edu*

31

31



University at Buffalo The State University of New York

TeamWork640x380px.png

## Tools & Resources

- ✓ Shared space – box
- ✓ Tracking
  - Spreadsheets
  - LMS – Learning Management System
- ✓ Project Management App
  - Planning
  - Tracking
  - Documenting
- ✓ QSA – Qualified Security Assessor
  - Phone calls
  - On-sight assessments

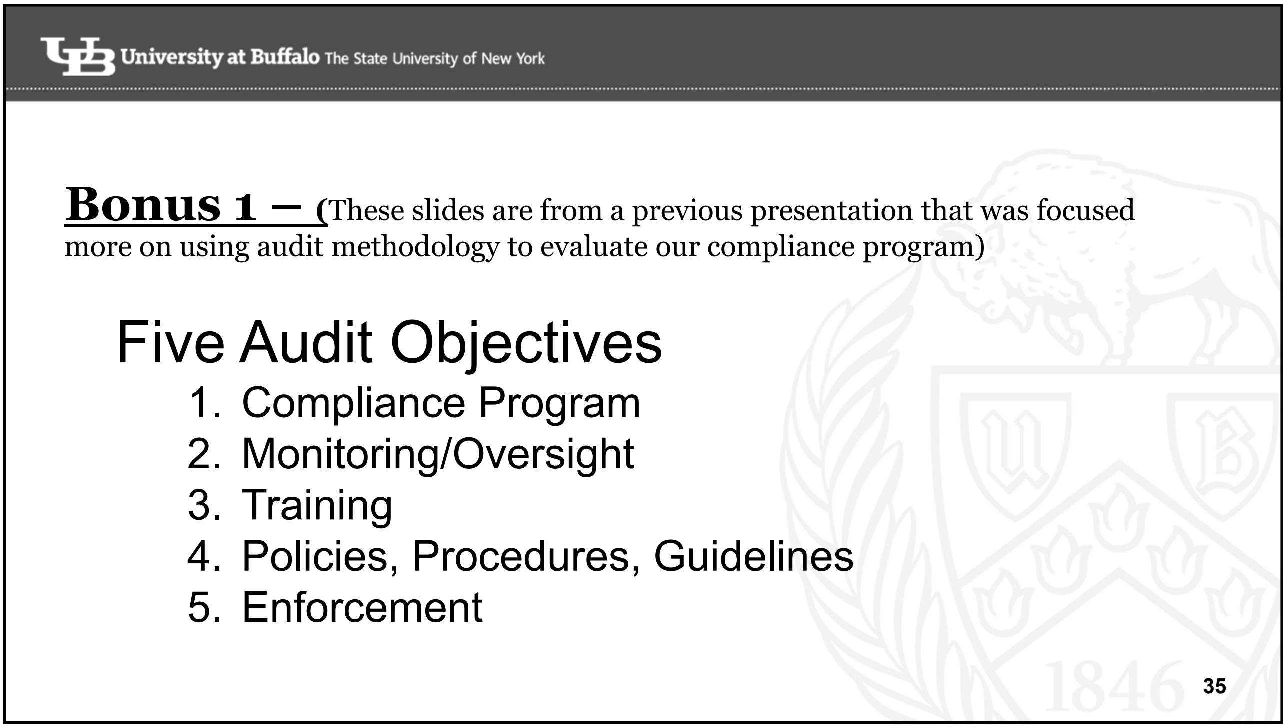
32

32

## Questions

Carolann G Lazarus, CISA, CCEP
IT Audit Manager,
University at Buffalo, SUNY
716-829-6947
lazarus@buffalo.edu

# BONUS

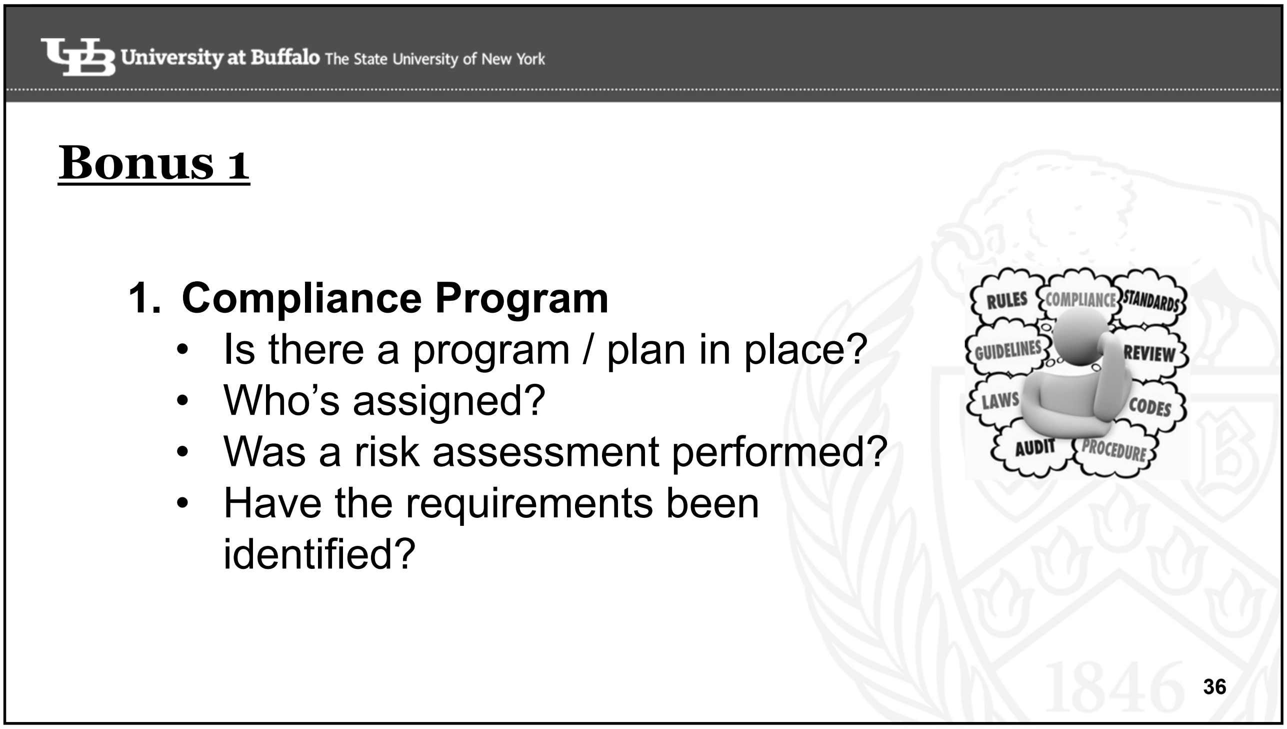


University at Buffalo The State University of New York

**Bonus 1 – (**These slides are from a previous presentation that was focused more on using audit methodology to evaluate our compliance program)

## Five Audit Objectives

1. Compliance Program
2. Monitoring/Oversight
3. Training
4. Policies, Procedures, Guidelines
5. Enforcement



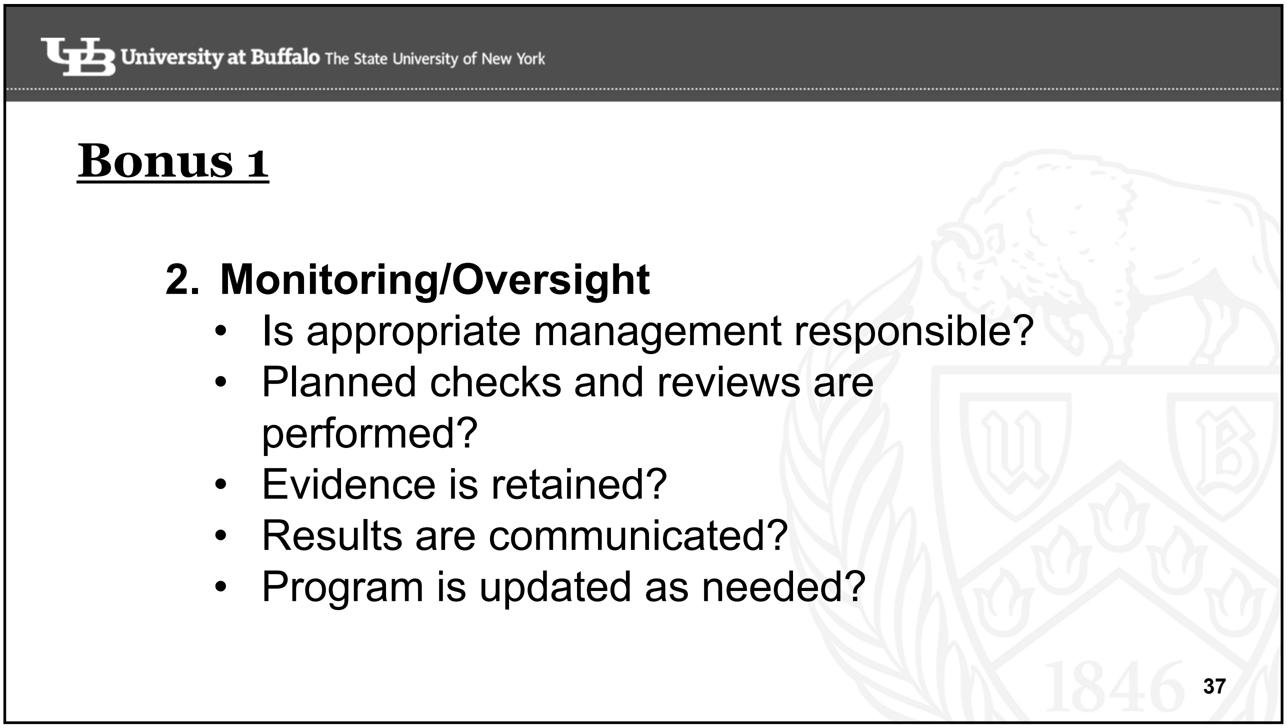
University at Buffalo The State University of New York

## Bonus 1

**1. Compliance Program**

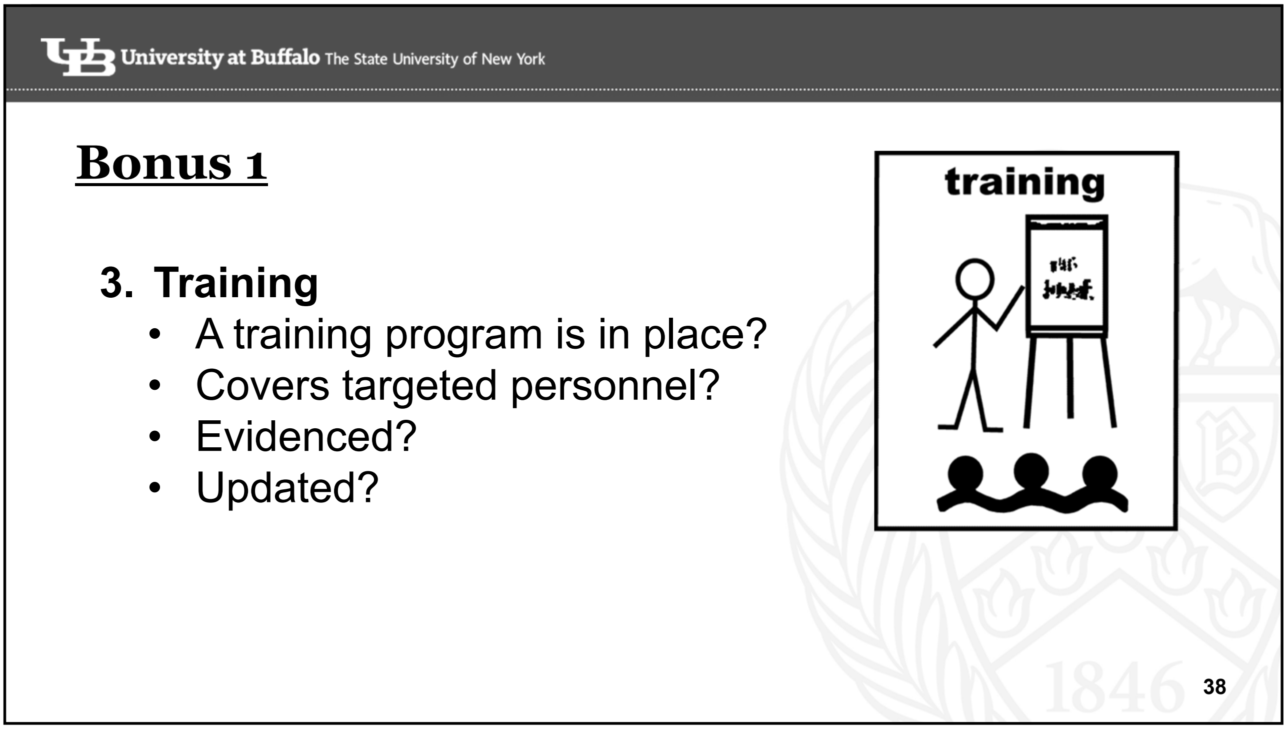
- Is there a program / plan in place?
- Who’s assigned?
- Was a risk assessment performed?
- Have the requirements been identified?

RULES
COMPLIANCE
STANDARDS
GUIDELINES
REVIEW
LAWS
CODES
AUDIT
PROCEDURE



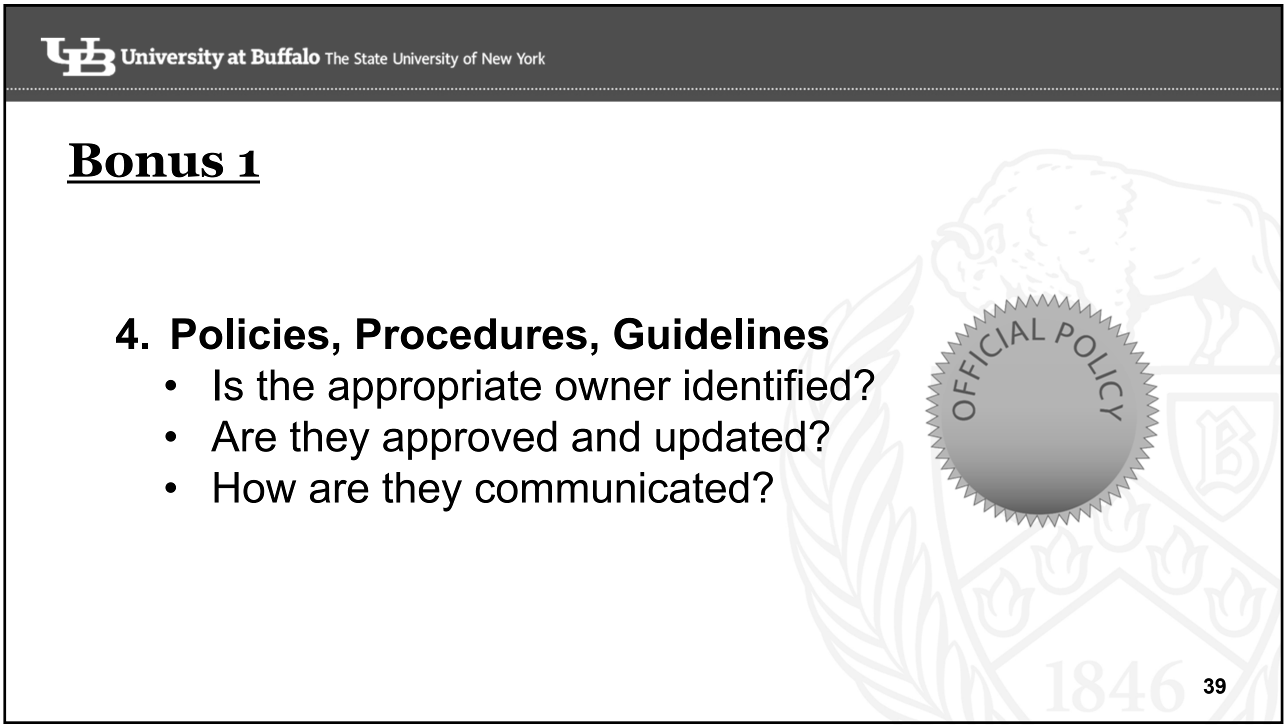
## Bonus 1

2. **Monitoring/Oversight**
   - Is appropriate management responsible?
   - Planned checks and reviews are performed?
   - Evidence is retained?
   - Results are communicated?
   - Program is updated as needed?



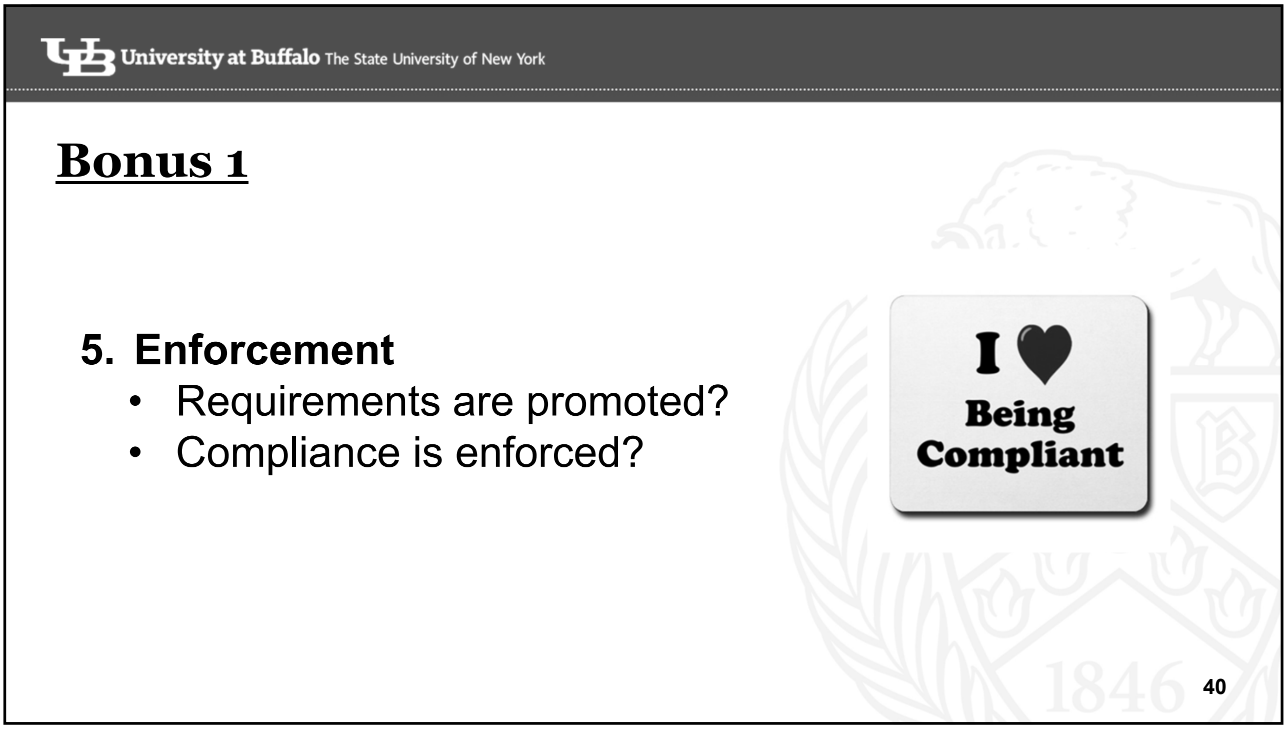
## Bonus 1

3. **Training**
   - A training program is in place?
   - Covers targeted personnel?
   - Evidenced?
   - Updated?



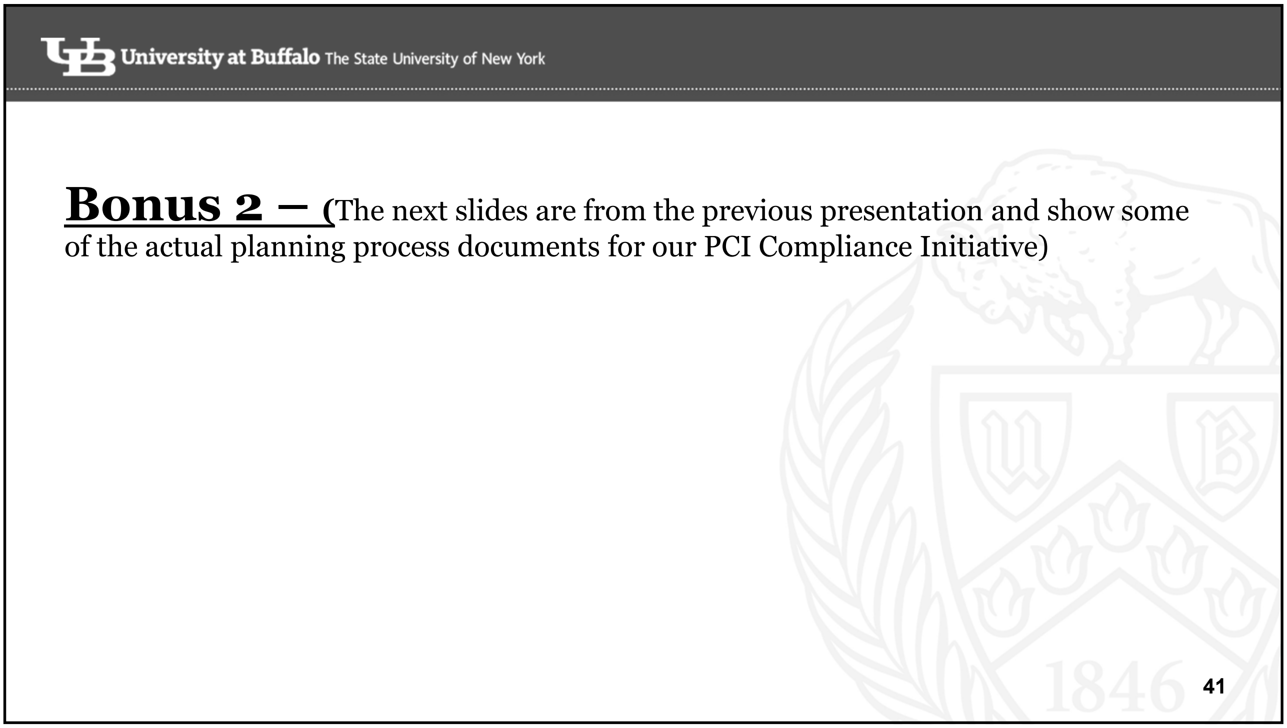
## Bonus 1

4. **Policies, Procedures, Guidelines**
   - Is the appropriate owner identified?
   - Are they approved and updated?
   - How are they communicated?



## Bonus 1

5. **Enforcement**
   - Requirements are promoted?
   - Compliance is enforced?

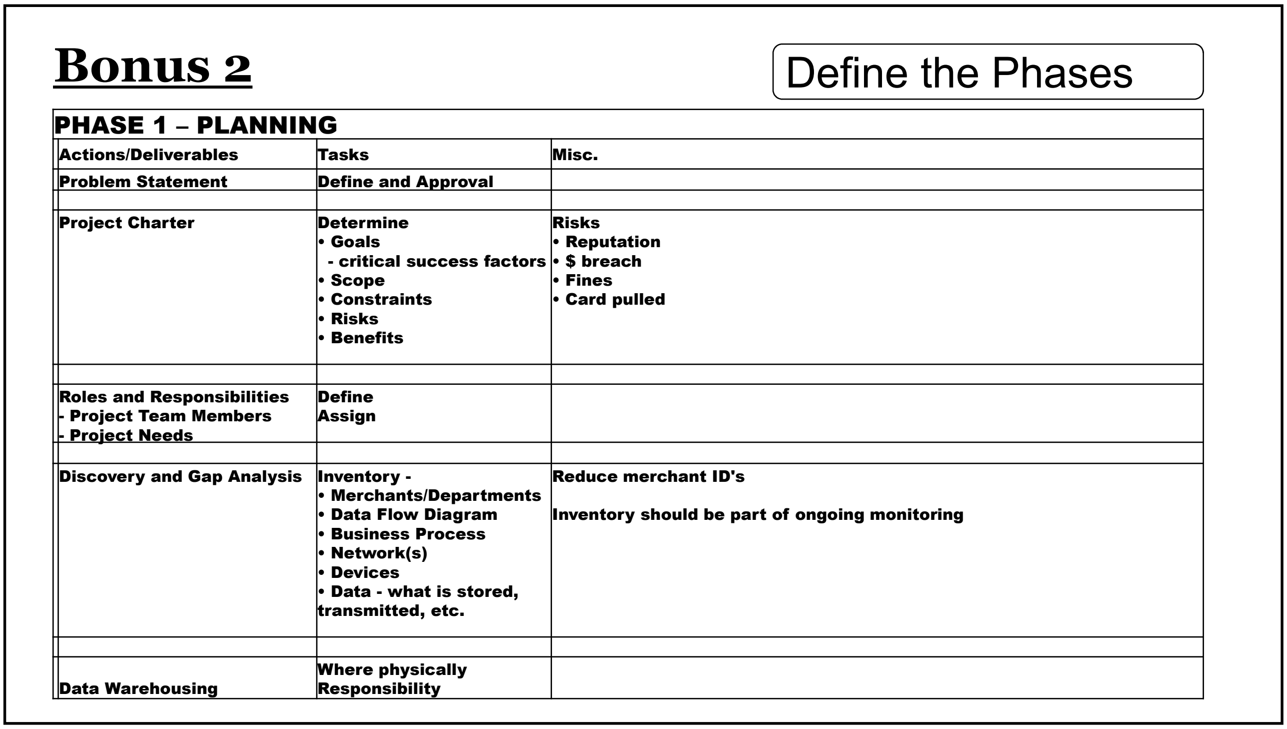


University at Buffalo The State University of New York

**Bonus 2 – (**The next slides are from the previous presentation and show some of the actual planning process documents for our PCI Compliance Initiative)

41

41



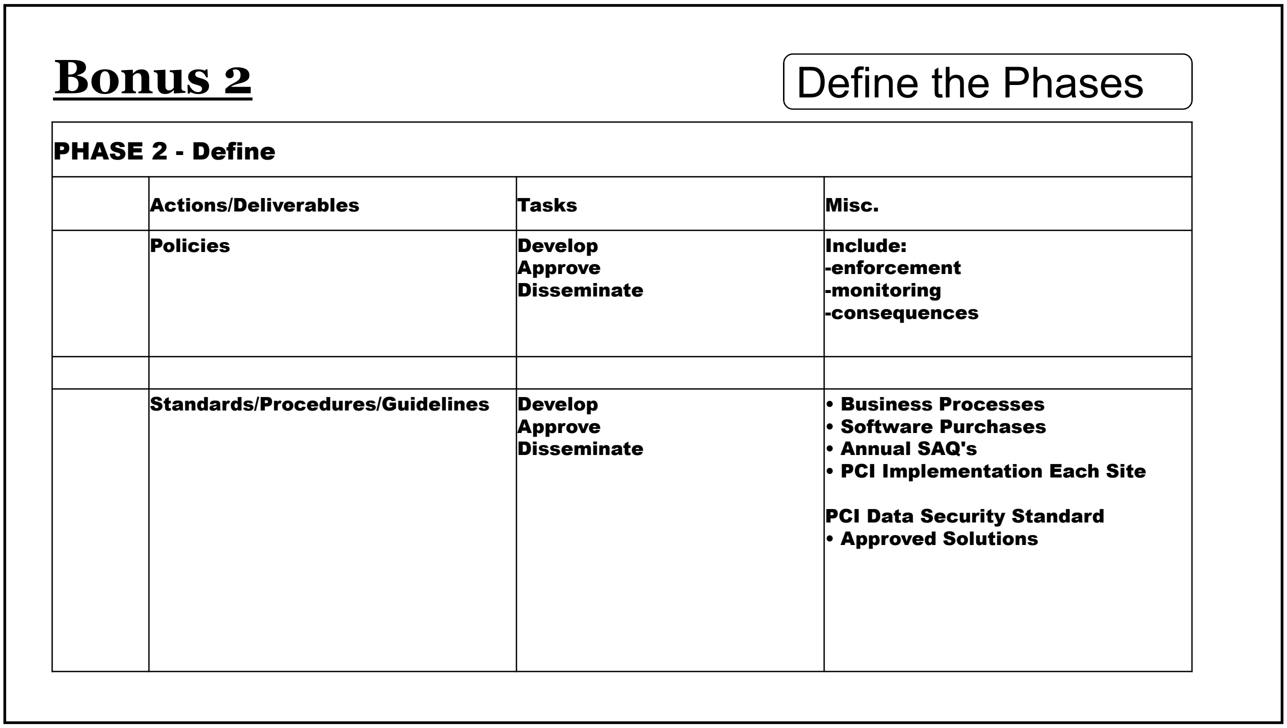
## Bonus 2

Define the Phases

**PHASE 1 – PLANNING**

| Actions/Deliverables | Tasks | Misc. |
|---|---|---|
| Problem Statement | Define and Approval | |
| | | |
| Project Charter | Determine<br>• Goals<br>- critical success factors<br>• Scope<br>• Constraints<br>• Risks<br>• Benefits | Risks<br>• Reputation<br>• $ breach<br>• Fines<br>• Card pulled |
| | | |
| Roles and Responsibilities<br>- Project Team Members<br>- Project Needs | Define<br>Assign | |
| | | |
| Discovery and Gap Analysis | Inventory -<br>• Merchants/Departments<br>• Data Flow Diagram<br>• Business Process<br>• Network(s)<br>• Devices<br>• Data - what is stored, transmitted, etc. | Reduce merchant ID's<br>Inventory should be part of ongoing monitoring |
| | | |
| Data Warehousing | Where physically<br>Responsibility | |

42

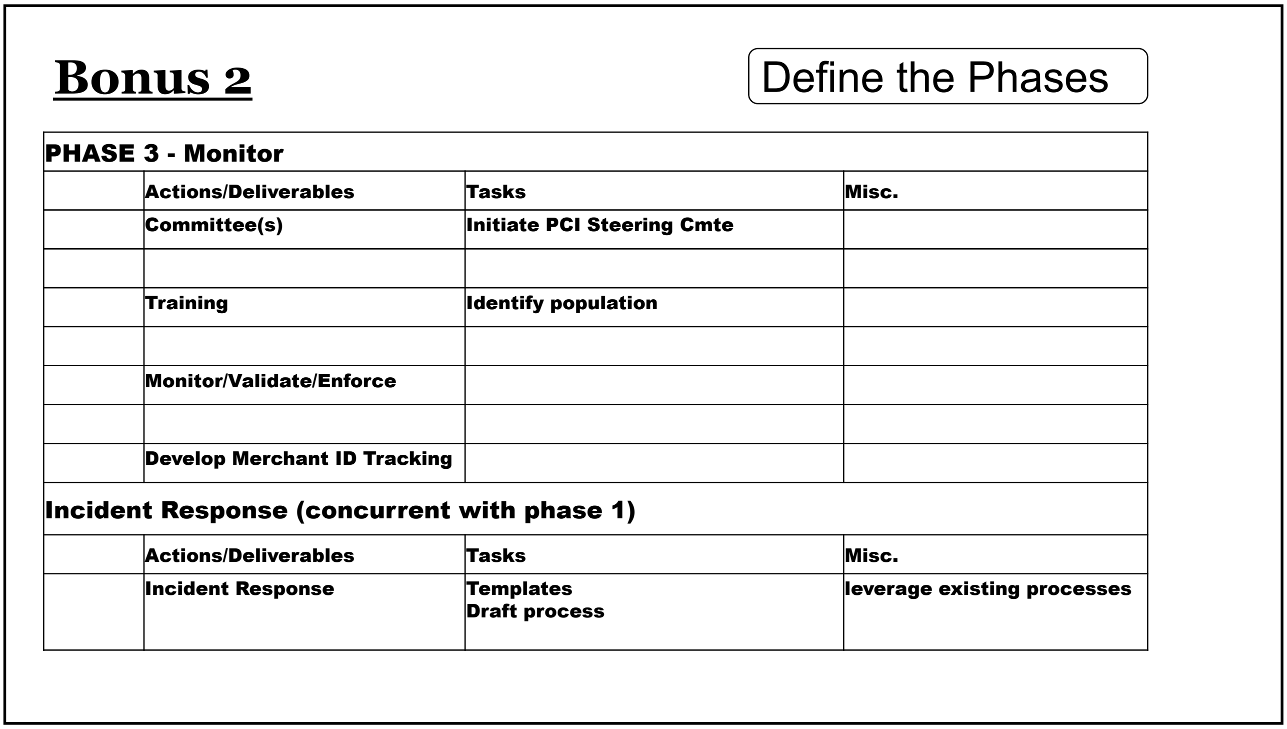


# Bonus 2

Define the Phases

| PHASE 2 - Define | | | |
|---|---|---|---|
| | Actions/Deliverables | Tasks | Misc. |
| | Policies | Develop<br>Approve<br>Disseminate | Include:<br>-enforcement<br>-monitoring<br>-consequences |
| | | | |
| | Standards/Procedures/Guidelines | Develop<br>Approve<br>Disseminate | • Business Processes<br>• Software Purchases<br>• Annual SAQ's<br>• PCI Implementation Each Site<br>PCI Data Security Standard<br>• Approved Solutions |

43



# Bonus 2

Define the Phases

| PHASE 3 - Monitor | | | |
|---|---|---|---|
| | Actions/Deliverables | Tasks | Misc. |
| | Committee(s) | Initiate PCI Steering Cmte | |
| | | | |
| | Training | Identify population | |
| | | | |
| | Monitor/Validate/Enforce | | |
| | | | |
| | Develop Merchant ID Tracking | | |

| Incident Response (concurrent with phase 1) | | | |
|---|---|---|---|
| | Actions/Deliverables | Tasks | Misc. |
| | Incident Response | Templates<br>Draft process | leverage existing processes |

44

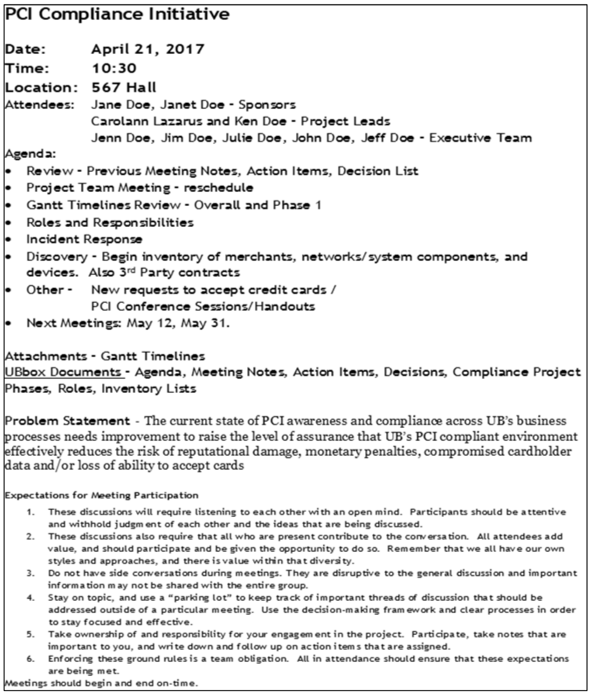
## Bonus 2

Meetings

- ✓ Frequency
- ✓ Documented Agendas
- ✓ Written Minutes
- ✓ Action Items Spreadsheet
- ✓ Decision List
- ✓ Parking Lot

## Bonus 2

Meetings - Agenda



**PCI Compliance Initiative**

**Date:** April 21, 2017
**Time:** 10:30
**Location:** 567 Hall
Attendees: Jane Doe, Janet Doe - Sponsors
Carolann Lazarus and Ken Doe - Project Leads
Jenn Doe, Jim Doe, Julie Doe, John Doe, Jeff Doe - Executive Team

Agenda:

- Review - Previous Meeting Notes, Action Items, Decision List
- Project Team Meeting - reschedule
- Gantt Timelines Review - Overall and Phase 1
- Roles and Responsibilities
- Incident Response
- Discovery - Begin inventory of merchants, networks/system components, and devices. Also 3rd Party contracts
- Other - New requests to accept credit cards / PCI Conference Sessions/Handouts
- Next Meetings: May 12, May 31.

Attachments - Gantt Timelines
UBbox Documents - Agenda, Meeting Notes, Action Items, Decisions, Compliance Project Phases, Roles, Inventory Lists

**Problem Statement** - The current state of PCI awareness and compliance across UB's business processes needs improvement to raise the level of assurance that UB's PCI compliant environment effectively reduces the risk of reputational damage, monetary penalties, compromised cardholder data and/or loss of ability to accept cards

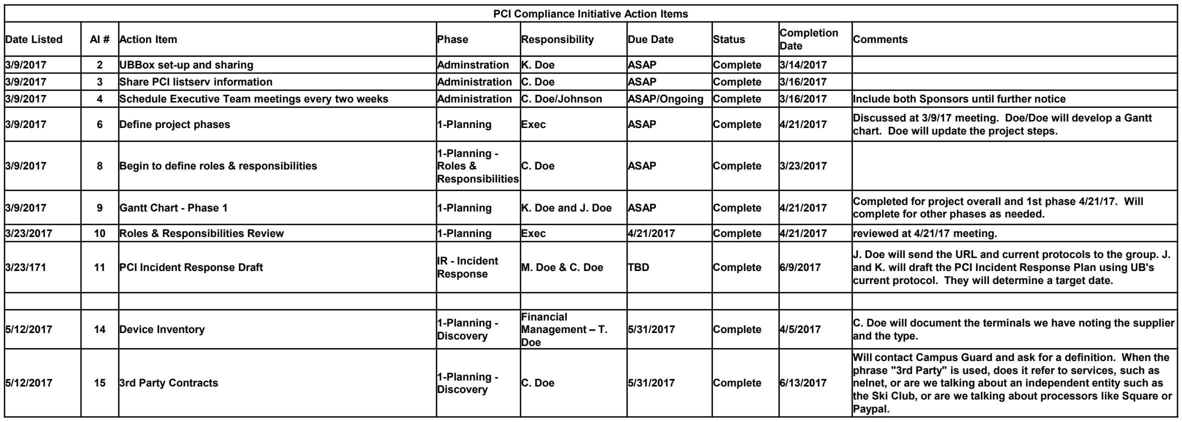
Expectations for Meeting Participation

1. These discussions will require listening to each other with an open mind. Participants should be attentive and withhold judgment of each other and the ideas that are being discussed.
2. These discussions also require that all who are present contribute to the conversation. All attendees add value, and should participate and be given the opportunity to do so. Remember that we all have our own styles and approaches, and there is value within that diversity.
3. Do not have side conversations during meetings. They are disruptive to the general discussion and important information may not be shared with the entire group.
4. Stay on topic, and use a "parking lot" to keep track of important threads of discussion that should be addressed outside of a particular meeting. Use the decision-making framework and clear processes in order to stay focused and effective.
5. Take ownership of and responsibility for your engagement in the project. Participate, take notes that are important to you, and write down and follow up on action items that are assigned.
6. Enforcing these ground rules is a team obligation. All in attendance should ensure that these expectations are being met.

Meetings should begin and end on-time.

## Bonus 2

## Meetings - Action List

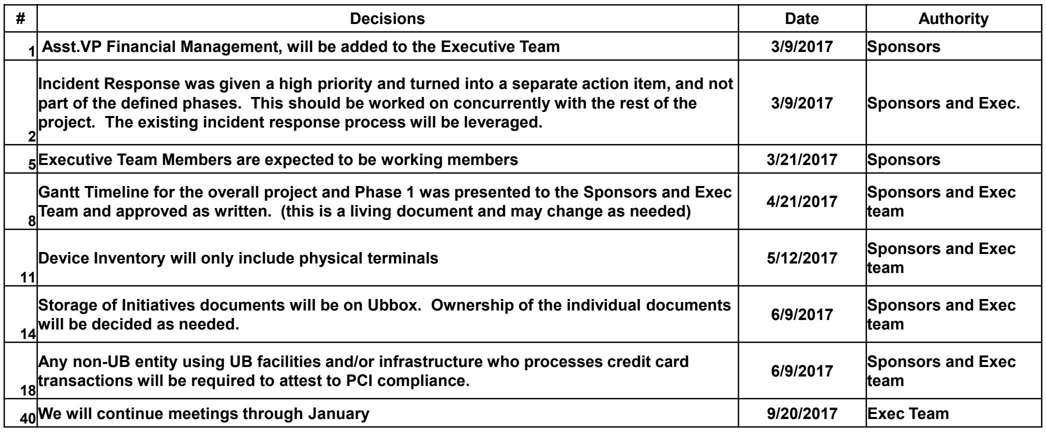


| PCI Compliance Initiative Action Items | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date Listed | AI # | Action Item | Phase | Responsibility | Due Date | Status | Completion Date | Comments |
| 3/9/2017 | 2 | UBBox set-up and sharing | Adminstration | K. Doe | ASAP | Complete | 3/14/2017 | |
| 3/9/2017 | 3 | Share PCI listserv information | Administration | C. Doe | ASAP | Complete | 3/16/2017 | |
| 3/9/2017 | 4 | Schedule Executive Team meetings every two weeks | Administration | C. Doe/Johnson | ASAP/Ongoing | Complete | 3/16/2017 | Include both Sponsors until further notice |
| 3/9/2017 | 6 | Define project phases | 1-Planning | Exec | ASAP | Complete | 4/21/2017 | Discussed at 3/9/17 meeting. Doe/Doe will develop a Gantt chart. Doe will update the project steps. |
| 3/9/2017 | 8 | Begin to define roles & responsibilities | 1-Planning - Roles & Responsibilities | C. Doe | ASAP | Complete | 3/23/2017 | |
| 3/9/2017 | 9 | Gantt Chart - Phase 1 | 1-Planning | K. Doe and J. Doe | ASAP | Complete | 4/21/2017 | Completed for project overall and 1st phase 4/21/17. Will complete for other phases as needed. |
| 3/23/2017 | 10 | Roles & Responsibilities Review | 1-Planning | Exec | 4/21/2017 | Complete | 4/21/2017 | reviewed at 4/21/17 meeting. |
| 3/23/171 | 11 | PCI Incident Response Draft | IR - Incident Response | M. Doe & C. Doe | TBD | Complete | 6/9/2017 | J. Doe will send the URL and current protocols to the group. J. and K. will draft the PCI Incident Response Plan using UB's current protocol. They will determine a target date. |
| | | | | | | | | |
| 5/12/2017 | 14 | Device Inventory | 1-Planning - Discovery | Financial Management – T. Doe | 5/31/2017 | Complete | 4/5/2017 | C. Doe will document the terminals we have noting the supplier and the type. |
| 5/12/2017 | 15 | 3rd Party Contracts | 1-Planning - Discovery | C. Doe | 5/31/2017 | Complete | 6/13/2017 | Will contact Campus Guard and ask for a definition. When the phrase "3rd Party" is used, does it refer to services, such as nelnet, or are we talking about an independent entity such as the Ski Club, or are we talking about processors like Square or Paypal. |

47

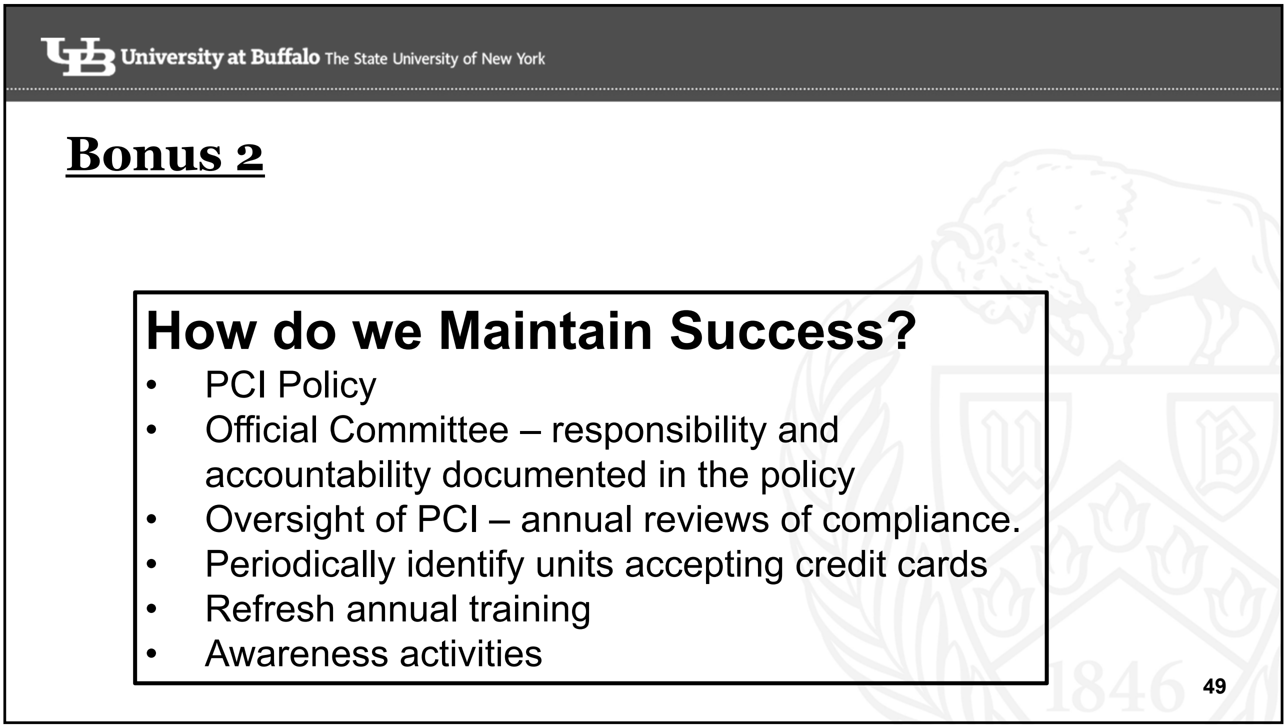
## Bonus 2

## Meetings -Decision List



| # | Decisions | Date | Authority |
|---|---|---|---|
| 1 | Asst.VP Financial Management, will be added to the Executive Team | 3/9/2017 | Sponsors |
| 2 | Incident Response was given a high priority and turned into a separate action item, and not part of the defined phases. This should be worked on concurrently with the rest of the project. The existing incident response process will be leveraged. | 3/9/2017 | Sponsors and Exec. |
| 5 | Executive Team Members are expected to be working members | 3/21/2017 | Sponsors |
| 8 | Gantt Timeline for the overall project and Phase 1 was presented to the Sponsors and Exec Team and approved as written. (this is a living document and may change as needed) | 4/21/2017 | Sponsors and Exec team |
| 11 | Device Inventory will only include physical terminals | 5/12/2017 | Sponsors and Exec team |
| 14 | Storage of Initiatives documents will be on Ubbox. Ownership of the individual documents will be decided as needed. | 6/9/2017 | Sponsors and Exec team |
| 18 | Any non-UB entity using UB facilities and/or infrastructure who processes credit card transactions will be required to attest to PCI compliance. | 6/9/2017 | Sponsors and Exec team |
| 40 | We will continue meetings through January | 9/20/2017 | Exec Team |

48



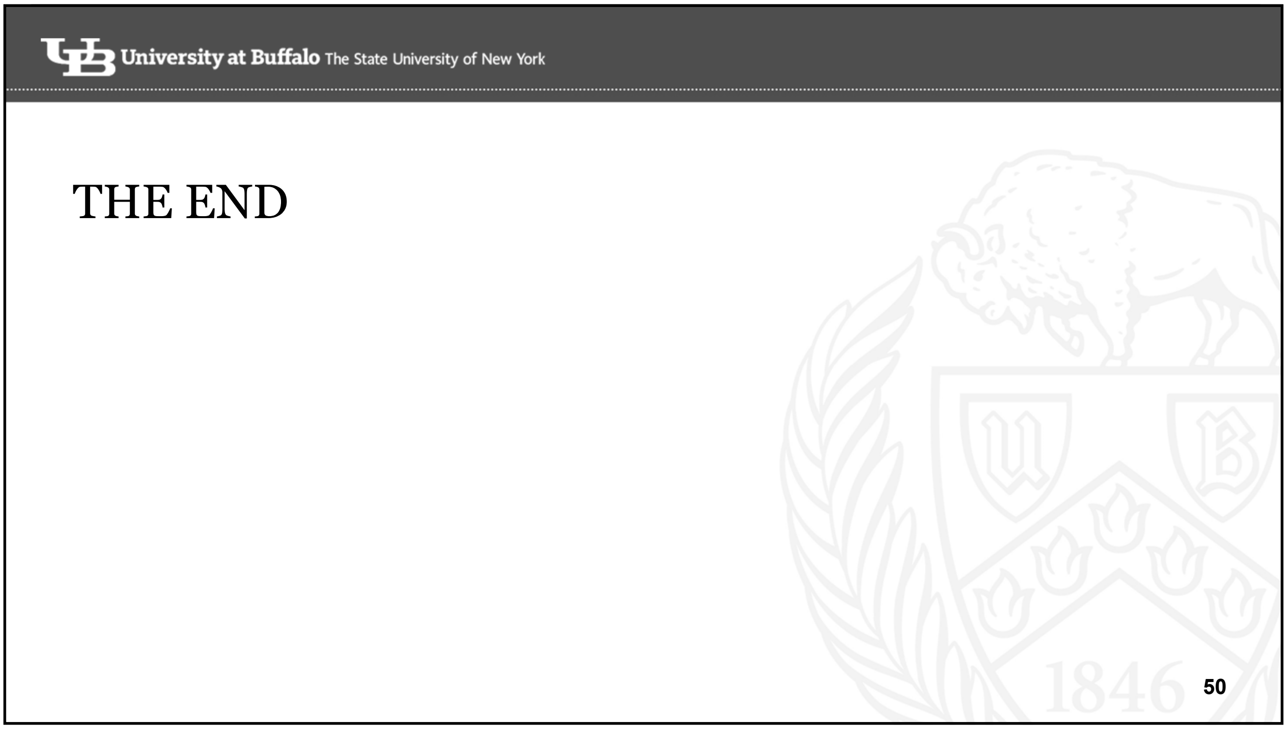
## Bonus 2

### How do we Maintain Success?

- PCI Policy
- Official Committee – responsibility and accountability documented in the policy
- Oversight of PCI – annual reviews of compliance.
- Periodically identify units accepting credit cards
- Refresh annual training
- Awareness activities

49

49



THE END

50

50