A University Path to Sustainable PCI Compliance

Reducing Scope, Reducing Risk

January 28, 2026

CAMPUSGUARD®

Stanford UNIVERSITY IT | Information Security Office

Presenters

- Shawn Kim
  Director of Cybersecurity Governance, Risk, and Compliance; Information Security Office
  Stanford University
- David Gundrum
  QSA, CISSP; Security Advisor
  CampusGuard
- Katie Johnson
  PCIP; Manager Operations Support,
  CampusGuard

Session Objectives

PCI Compliance

Learn how Stanford tackled PCI challenges and what worked (and what didn’t) in a real-world campus environment

Reducing Scope

Discover practical ways to shrink your organization’s PCI scope and make compliance less overwhelming

Recommendations

Walk away with clear recommendations to build stronger governance and simplify processes

Complex Environment

Lack of resources

376 campus merchants (and counting)

OPEN

Competing responsibilities

Vendors/Third-Party Service Providers

Evolving DSS requirements

Various Payment Technologies

(card-present, ecommerce, phone transactions, kiosks, etc.)

Decentralized IT

PCI Compliance Program

Understanding the merchant environments

2021

- Stanford Information Security Office (ISO) and Merchant Services teams take over joint ownership of the University's PCI Compliance Program
- QSA compliance assessment to understand all campus merchants who are taking payments and their current payment methods
- Areas of non-compliance identified
- Recommendations to reduce scope / reduce risk
- Prioritized roadmap to compliance

Remediation

Step 1: Reduce overall PCI scope (reviewing all SAQ A-EP, B-IP, B, C and SAQ D merchants)

- Reviewed payment methods, payment flows, and transaction volume
- Explored alternative options and/or vendors
- Deployed P2PE equipment where possible for card-present
- Transitioned to outsourced, compliant ecommerce vendors

Goal

Decommission the PCI network

Three Phases

1

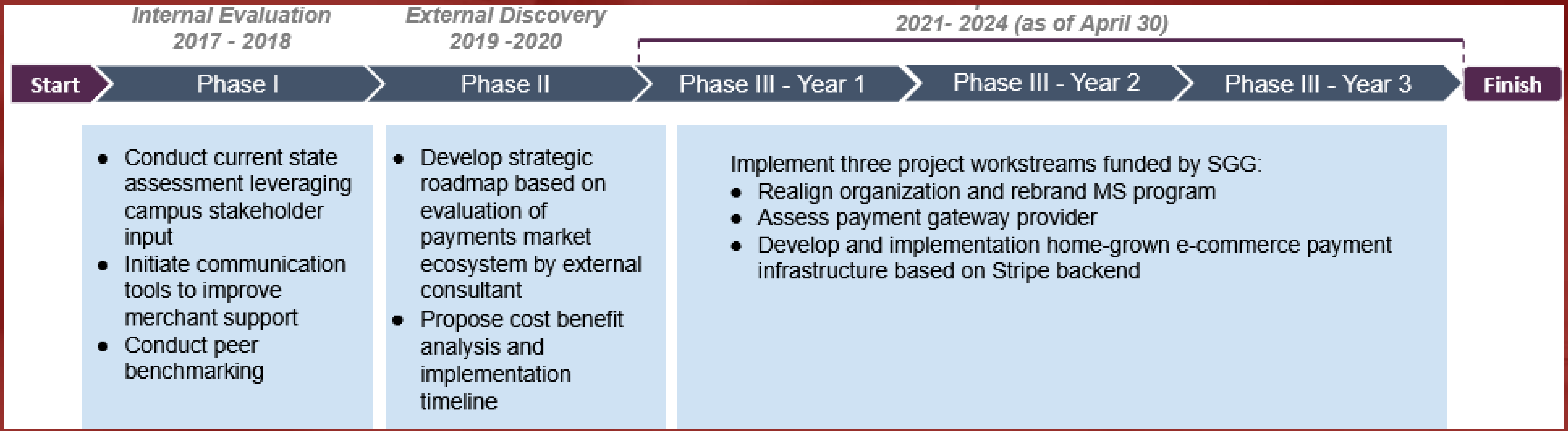
Phase I: Internal Assessment/Discovery (2017–2018)

2

Phase II: External Assessment: Market Scan & Roadmap Development (2019–2020)

3

Phase III: Implementation & UniRev Launch (2021–2024)



Internal Evaluation 2017 - 2018
External Discovery 2019 -2020
2021- 2024 (as of April 30)
Start
Phase I
Phase II
Phase III - Year 1
Phase III - Year 2
Phase III - Year 3
Finish

- Conduct current state assessment leveraging campus stakeholder input
- Initiate communication tools to improve merchant support
- Conduct peer benchmarking

- Develop strategic roadmap based on evaluation of payments market ecosystem by external consultant
- Propose cost benefit analysis and implementation timeline

Implement three project workstreams funded by SGG:

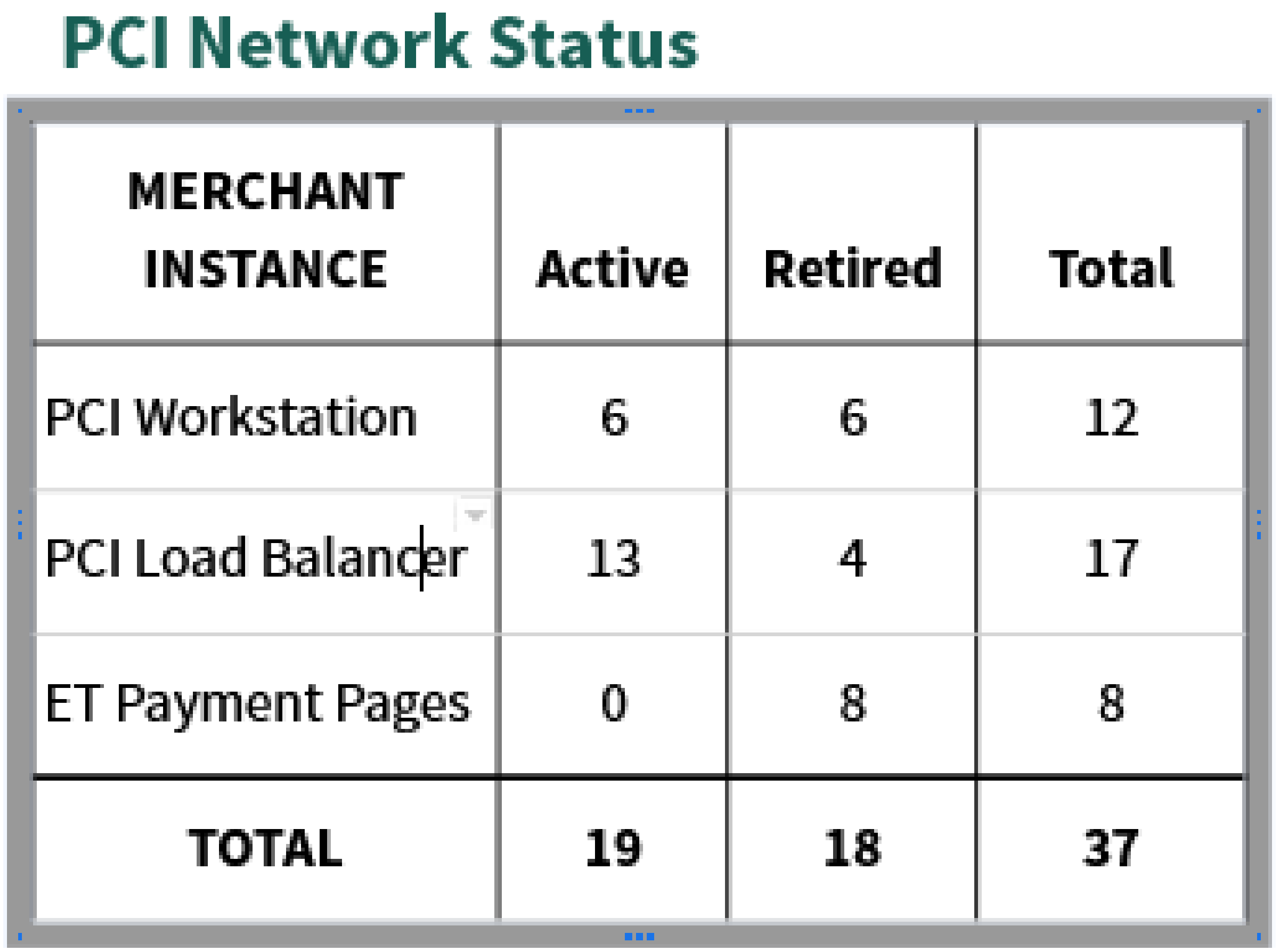
- Realign organization and rebrand MS program
- Assess payment gateway provider
- Develop and implementation home-grown e-commerce payment infrastructure based on Stripe backend

Decommission PCI network infrastructure

CardinalPay (UniRev) runs on the Stanford open network

Each merchant was redirected to a dedicated hosted merchant page for defined payment streams

Customers interface with individual Stripe accounts that are decentrally accessed and centrally managed



PCI Network Status

MERCHANT INSTANCE	Active	Retired	Total
PCI Workstation	6	6	12
PCI Load Balancer	13	4	17
ET Payment Pages	0	8	8
TOTAL	19	18	37

Scope Reduction

Reducing risk and compliance burden

2024

➢ **Merchant Process Changes**

- All merchants now able to attest using reduced scope SAQs (SAQ P2PE and SAQ A)

➢ **CardinalPay**

- University-developed solution
- Consolidating available payment methods
- Needs analysis with each merchant

➢ **PCI Network Disabled**

- Reducing expensive technology costs
- Eliminating compliance requirements like pen testing, logging, etc.

Annual Compliance Calendar

Merchant Surveys

May

Identify any changes/challenges

Merchant Assessments

May

Selected sample of merchants

PCI Awareness Training

May

Primary launch

Ongoing effort

Device Inventory/ Inspections

Ongoing

Defined frequency based on overall risk

Ecommerce Inventory

Keeping up to date/tracking new online payment sites

Policy/Merchant Procedures

Annual review

Based on payment methods/processes

Vendor Oversight

Ongoing DRA process

Annual AOC collection

Responsibility Matrix

Incident Response Plan Testing

March

PCI-focused exercise

ASV Vulnerability Scanning

Quarterly

External scans

Self-Assessment Questionnaires

October

Annual completion by individual merchants

Annual Attestation of Compliance

December

Overall attestation to the acquiring banks

Addressing VoIP

Initial Assessment

- Conducting review of all merchants taking payments over the phone
- Evaluating transactions/volume
- Identifying alternative payment methods (i.e., ecommerce)

Solution Evaluation

- Secure VoIP Network
- Mobile phones
- IVR/DTMF solutions
- Vendor analysis

Implementation

Lessons Learned

- **Uncovering Hidden Risks**
  Finding out from merchants (after the fact) about different vendors in use, planned changes, storing data on paper, taking payments on behalf of customers, etc. Build relationships and meet with merchants in person ongoing

- **Clearly defining roles and responsibilities**
  Outlining merchant responsibilities and identifying communication channels

- **Third-Party Service Provider Oversight**
  DRA process – involving teams early in purchasing, reviewing compliance documentation, meeting to explain requirements, evaluating shared responsibilities

Lessons Learned

- **Balancing Risk and Business Needs**

  Clearly define how much risk the organization can accept

- **Leadership Buy-in and Support**

  Ensuring leadership understands the risk of non-compliance

- **Evolving Requirements**

  PCI DSS v4.0.1 – new requirements (full ecommerce review, etc.)

- **Documentation**

  Updating policy/procedure to align with current practices

Looking Forward

- Maturing the program
- Compliance business as usual
- Identify ways to streamline tasks (training)
- Merchant responsibilities – SAQs, verifying documentation, inspections, etc.
- Being more proactive than reactive with merchant changes
- Communication – Do merchants know who to contact and when?
- Prioritizing third-party oversight

Recommendations

Start with a clear goal in mind.

Understand current state.

Obtain leadership buy-in and support.

Build relationships with the merchants and bridge gaps across functional areas.

Weigh options carefully and prioritize risk.

It will take time. PCI DSS is a cyclical improvement process.

Thank You

CAMPUSGUARD®

Stanford UNIVERSITY IT | Information Security Office