A CASE STUDY

Maintaining PCI Compliance

WHO

Research University
- 70+ merchant accounts
- 6+ storage locations
- 2 payment applications
- 5+ PCI service providers used
- PCI Service Provider

WHAT

Maintain PCI Compliance

WHY

System upgrades
Change in processes
Increased maintenance

HOW

PCI DSS Scoping, PCI DSS Preparedness Assessment, Remediation, Validation

OVERVIEW

HALOCK partners with a research university to conduct a comprehensive PCI DSS project to ensure compliance. With applications continually being upgraded, processes amended, and the anticipation of PCI DSS v4.0, the institution needed to review how these changes impact their compliance.

Over a 6-month time frame, HALOCK manages a wholistic approach which includes:

- PCI Program Planning
- PCI Scope Validation
- PCI Preparedness Assessment
- PCI Remediation Efforts
- PCI Compliance Validation

PLANNING

The key to a successful project is proper planning. HALOCK develops the project and communications plan, collaborates with the university to set scheduling, resources, and review maintenance activities and controls.

SCOPE

The institution conducts their annual credit card processing survey which was developed with HALOCK and implemented for the past 10 years to ensure:

- Only approved acceptance channels and third parties are used.
- No additional processes are added without the team's knowledge and approval.

HALOCK facilitates scope validation for the university by collecting and reviewing up-to-date scoping information such as:

- Hardware and Software Inventories
- Network Layout and Diagrams
- Cardholder Data Flows
- Credit Card Acceptance Channels
- Cardholder Storage Repositories
- Payment Applications
- Third-Party Service Providers
- Vulnerability and Penetration Test Results

ASSESSMENT

The interview sessions typically yield a total of 311 Compliance Data Points (CDPs) applicable for PCI compliance, which need to be in place and documented.

HALOCK works with the university to facilitate all expected testing procedures for applicable PCI DSS Self-Assessment Questionnaires (SAQs).

REMEDIATION

Challenges identified are usually related to ongoing maintenance and application upgrades.

TYPICAL FINDINGS

Operational follow-up confirmations
Technical
Documentation

TYPICAL IMPROVEMENTS

Documentation
Processes
Training

As HALOCK reviews items and provides feedback, the university works with teams to address any gaps identified in order to demonstrate full PCI DSS compliance. **By the end of the preparedness assessment, the institution is 100% compliant.**

COMPLIANCE VALIDATION

This university still validates PCI DSS compliance through SAQs. HALOCK and the university collaboratively complete an SAQ-D for service providers and merchants and corresponding AOCs (Attestation of Compliance) as it is both a PCI Merchant and Service Provider.