

**PCI COMPLIANCE FOR HIGHER EDUCATION
BEST PRACTICES CHECKLIST**

Presented By:

The Treasury Institute for Higher Education

&

AmbironTrustWave

Executive Summary

This checklist is intended to help guide a university through some of the preliminary stages of their PCI Compliance efforts. While no two environments tend to be the same, this checklist details many of the effective and successful initiatives that have been launched by various universities, many who presented on their experiences at the Treasury Institute's Symposium regarding PCI DSS Obstacles in Higher Education. As a caveat, this checklist will not guarantee compliance, nor will it address every issue that may arise during this process. However, it should provide an initial outline for approaching the PCI issue and helpful advice throughout the process.

Table of Contents

1.	Establishing Buy-In.....	3
2.	Assessing Your Current Environment.....	6
3.	Segmenting Your Network.....	8
4.	Ensuring Third Party Compliance.....	9
5.	Training, Development & Education.....	10

1. Establishing Buy-in

- a. Gather relevant information to present to upper management
 - i. PCI Requirements and other regulatory mandate information
 - ii. Articles/Headlines discussing university breaches
 - iii. Liability costs (which may include any or all of the following):
 - 1. Reputation
 - 2. Fines
 - 3. Card Re-Issuance fees
 - 4. Forensic investigation costs
 - 5. Costs of notifying victims
 - 6. Remediation costs
 - iv. Operating Costs - (Increased operating costs may include):
 - 1. Requirements for quarterly scans
 - 2. An increased need for network security hardware
 - 3. Potential need for staff to monitor networks

- b. Determine resources needed for project
 - i. Have plan for requesting resources from upper management
 - ii. Determine source of funding for increased operating costs (these costs may include):
 - 1. Immediate remediation needs
 - 2. Migrating departments to approved applications
 - 3. Changing network configurations to segment valuable information assets.

- c. Identify an individual in upper management to support the project
 - i. Obtain/Create message from CFO or Financial Dean(s) explaining university's commitment to PCI compliance
 - 1. Send to department heads/business managers
 - a. *Assign accountability to them making them responsible for all PCI requirements*
 - 2. Introduce project manager
 - 3. Identify stakeholders
 - 4. Inform stakeholders that PCI DSS is their responsibility
 - a. *Include that compliance is a community issue*
 - 5. Set realistic date for completion of compliance project
 - 6. Explain consequences of non-compliance
 - a. *Deactivation of merchants not compliant by due date*
 - b. *Fines if breached*
 - c. *Department on their own if breached*

- d. Create a full-time position to manage compliance or assign a compliance-project manager
 - i. Employee should report regularly on progress and issues to upper-management representative
 - ii. Responsibilities should include developing communication campaign to inform and engage departments

- e. Form a card payments review board
 - i. Should include representatives from finance/treasury, IT/IS, Legal, Internal Audit, and possibly others, regardless of how these departments are structured.
 - ii. Review departmental progress towards, and maintenance of, PCI compliance
 - iii. Create or define process for reviewing department requests for payment card acceptance
 - 1. Create an administrative e-commerce guide
 - 2. Explain university e-commerce policies and procedures
 - 3. Add PCI compliance language to all relevant contracts (more on third party issues later)
 - iv. Define central management for all payment card acceptance (e.g. At one institution, the Associate Controller handles all card payments management)
 - 1. Explore handling payments and cardholder information outside university network
 - 2. Define merchant responsibilities versus central management responsibilities
 - 3. Identify exceptions
 - a. For example, one institution developed a centralized payment management service
 - i. *Considered building, but buying was more cost effective*
 - ii. *"Online cash register"*
 - iii. *Branded Web site redirects customers to hosted order page*
 - v. Create training program for payment card acceptance (more on this in the Training section)
 - 1. Establish buy-in and accountability for attendance, including department contacts and penalties (i.e. fines and removal of card acceptance privileges)
 - 2. One institution developed a PCI training road show that traveled to department meetings to inform merchants of changes

- vi. Inform stakeholders that cost of payment card acceptance will increase, by communicating “Risk Cost vs. Implementation Costs” (which may include some of the following):
 - 1. Risk Costs
 - a. Damage to Reputation / Brand
 - b. Fines
 - c. Card Re-Issuance fees
 - d. Forensic investigation costs
 - e. Costs of notifying victims
 - 2. Implementation / Remediation Costs
 - a. Quarterly network scans
 - b. Network security hardware
 - c. Migration to approved applications
 - 3. Determine allocation of above costs
- vii. Ensure expertise exists (either internally or hire outside assessor if necessary)
 - 1. Important, up-to-date information can be found at the following address:
<https://www.pcisecuritystandards.org/index.htm>
 - 2. Outside assessors have to be annually certified and should have up-to-date information.

2. *Assessing Your Current Environment*

- a. Meet with your acquiring bank to determine your appropriate merchant level. Some examples of level definitions are available at the following websites:
http://usa.visa.com/business/accepting Visa/ops_risk_management/cisp_merchants.html
https://sdp.mastercardintl.com/merchants/merchant_levels.shtml
- b. Examine IP addresses and merchant IDs to confirm merchants
- c. **Notify department heads of their accountability for their department's network infrastructure and information provided to compliance committee.**
- d. Have merchants/departments sign a contract identifying their accountability for PCI Compliance
- e. Identify department contact/resource for PCI scoping and accountability.
- f. Survey department heads to determine the following information:
 - i. Business and technical contact
 - ii. Current method of payment card processing
 - iii. Where site is hosted
 - iv. If they store payment card data and where
 - v. IP address and/or URL
 - vi. Understand payment card solutions currently in use (which may include some of the following):
 1. Hosted order pages
 2. Point-of-Sale (POS) systems
 3. Interactive Voice Response (IVR)
 4. Phone Orders
 5. Mail Order
- g. Determine pros and cons of departments accepting payment cards
 - i. What departments accept payment cards?
 - ii. Do they need to?
 - iii. Are there alternatives?
 1. Examples may include migrating processes to centrally managed system and appropriate solutions

- h.* Hire an outside assessor if necessary.
 - i. An outside assessor is **necessary** if an institution is a level 1 merchant or deemed high-risk by the card associations
 - ii. An outside assessor can assist in the development of policies and procedures.
 - iii. Find a list of Qualified Assessors at the following website:
https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm

- i.* If an institution is a Level 1, 2, or 3; they are **required** to hire a Qualified Independent Scan Vendor for quarterly network scans. A list of these vendors can be found at the following website:
https://www.pcisecuritystandards.org/resources/approved_scanning_vendors.htm
 - i. Identify high-risk network vulnerabilities across various merchant profiles and remediate these first. These high-risk network vulnerabilities can easily be determined by the quarterly scans.

- j.* Identify the various types of merchant profiles that are utilized on your campus, then develop pre-populated questionnaires for these different profiles
 - i. Identify high-risk merchants to handle first
 - ii. Develop remediation plans

- k.* Develop and implement any and all appropriate policies and procedures
 - i. Information Security Policy
 - ii. Incident Response Plan

3. Segmenting Your Network

- a. Identify the need for segmentation within the environment
 - i. Continue open access to university resources (which may include):
 - 1. Libraries
 - 2. Group Study
 - 3. Interest groups
 - ii. Segment and protect critical assets (which may include):
 - 1. Payment card information
 - 2. Social Security numbers
 - 3. Transcripts/grades
- b. Restrict access to segments that contain critical assets
 - i. Allow access on a “need-to-know” basis
 - ii. Build boundaries around segments (firewalls, IDS/IPS, etc.)

4. Ensuring Third Party Compliance

- a. **Contractually require that all third parties involved in credit card transactions meet all PCI security standards, and that they provide proof of compliance and efforts at maintaining ongoing compliance. Contract should:**
 - i. Include an acknowledgement that the third party is responsible for the security of any cardholder data that they process, transmit or store
 - ii. Proactively determine responsibilities in the event of a breach
 - iii. Discuss how the third party is addressing changes in their compliance status and how that can affect their future responsibilities
 - iv. Discuss how the third party is addressing changes in their environment which may also affect their compliance status and therefore their subsequent responsibilities in the event of a breach

- b. **A list of approved and certified service providers can be found at:**
http://www.usa.visa.com/download/business/accepting_visas_risk_management/cisp_List_of_CISP_Compliant_Service_Providers.pdf?it=il/business/accepting_visas_risk_management/cisp_service_providers.html|List%20of%20CISP-Compliant%20Service%20Providers

- c. **If using a payment application, confirm that the application adheres to Visa's Payment Application Best Practices (PABP).** A list of approved applications (including release and version numbers) can be found at the following website:
http://www.usa.visa.com/download/business/accepting_visas_risk_management/cisp_Validated_Payment_Applications.pdf

- d. Know and understand all outside parties that connect to your organization's network
 - i. Employ proper due diligence in admitting 3rd parties onto your network. Establish a process for incorporating and announcing 3rd parties linked to your network.
 - ii. Maintain and actively control a list of these parties
 - iii. Be prepared to communicate companies that are **removed** from this list.

5. *Training, Development and Education*

- a. Develop ongoing training programs to train employees on the PCI DSS and importance of compliance. (E.g. one institution holds annual “awareness” classes) Training should include and confirm understanding of the following:
 - i. The university’s security policies and procedures in addition to policies and programs on PCI and credit card acceptance
 - ii. The process for initiating payment card acceptance
 - iii. The process for requesting a merchant ID
 - iv. The incident response plan
 - 1. Define roles and responsibilities for affected parties
 - 2. Specify reporting requirements
 - v. **Require signature confirmation of the security policies**
- b. Establish and reiterate the importance of the program and the commitment to the training:
 - i. Require department heads or delegates to attend
 - ii. Provide regular e-mail notices and updates
- c. Communicate the consequences should an employee or department fail to follow written policies. Examples may include:
 - i. Deactivation of merchant accounts
 - ii. Possible fines
- d. Create and communicate using the centralized repository of resources for those accepting or starting to accept payment cards. Repository should include the following:
 - i. PCI DSS guidelines and updates
 - ii. Self-assessment questionnaire
 - iii. Policies and procedures
 - iv. Any template documents
 - v. Process to request payment card acceptance
 - vi. Support resources and contacts
 - vii. Incident Response Plan