Making Sense of the PCI Puzzle

A guide to organizing your merchant accounts on campus

Coalfire

Sponsored By: HigherOne

Contributors from Coalfire Systems, Inc.

Joseph Tinucci

Justin Orcutt

Eva Araya

The Big Picture

Universities are like small towns, with numerous merchants all operating within the school's boundaries. Among other things, universities allow credit and debit card transactions as a way of paying expenses such as tuition and fees, books, food and other services available on campus. On-campus merchants that accept credit cards include the bookstore, bursar's office, dining halls, athletic/performing arts tickets, concessions, libraries, campus security, vending machines and residence halls. There are dozens of other merchants on college campuses that can add value, increase revenues and effectively increase budgets. The downside is the risk to students' financial information, which is spread out and processed by several merchants.

Third-party merchants like Sodexo or Aramark can run several different services for universities and have their own cyber-security procedures, which takes some of the pressure off the university. Some merchants, however, are the university's direct responsibility. As such, the university should take special care to keep track of its merchants and the financial information they receive in all corners of its campus. Here's how to do it.

Part One: Identifying Your Merchants

The first step in protecting students' financial information and becoming PCI DSS compliant is to inventory and keep track of all merchants. We call this step a "needs assessment." You need to identify who the merchants are and where they're located on campus. You'll need to know what controls they have in place, which payment technology they use, and log Merchant IDs if you haven't already. It's also useful to track the annual volume of credit card transactions annually for scope reduction prioritization, which we'll cover a bit later in this document.

Tracking total transactions is essential to determining your university's merchant level, which ultimately determines the extent of PCI DSS controls you need to validate against. Acquiring banks identify universities as level 3 or 4 merchants, but there are a number of level 1 and level 2 universities throughout the country as well.

Level 3 and 4 merchants have the ability to conduct a Self Assessment Questionnaire (SAQ). However, these same universities often struggle to understand which SAQ to fill out, how many to complete, and how to manage their PCI DSS compliance program.

Properly inventorying your merchants will enable you to understand the needs of the university and your reporting requirements. If after the merchant inventory you still do not understand which SAQs to complete, consult with a Qualified Security Assessor (QSA) or your acquiring bank, which has the final say regarding which SAQ schedules you need to complete.

Once you understand how your merchants work, where they are located and the payment technology they use, you can begin to group them together and develop a more manageable program. This will help reduce risk and the chance of an incident.

Making Identification Easy with Needs Assessments

A needs assessment is a simple worksheet that helps you identify and assess the vulnerabilities of your merchants. Below is an example that allows you to identify the key parts of your PCI DSS compliance program. This will be used to consolidate merchants, identify payment technology risks, identify merchants where cost of compliance is too high and provide the backbone of your PCI DSS compliance program.

ORGANIZATION NAME	College Bookstore
MERCHANT DESCRIPTION	The bookstore is a university-owned facility that sells books, merchandise alumni apparel and more. The bookstore accepts payments for books, tutors, merchandise and ticket sales. It also has its own e-commerce site and merchant ID.
PRESUMED SAQ	SAQ D
JUSTIFICATION	The bookstore accepts payments through two primary channels: 1. Payment for books and apparel are performed as a card-present transaction processed through a standalone dial-out terminal; 2. Payments for ticket and events are accepted as either card-present transactions through a standalone dial-out terminal or through card-not-present transactions using a web service managed by <INSERT SERVICE PROVIDER>.
AFFECTED MIDS	5
POC	Merchant Contact Information
PAYMENT TECHNOLOGY	Dial-Out Terminal (MODEL #)
SPECIAL NOTES	The bookstore has installed a Risk Management Software solution to help with inventory, pricing and event management. The software has a payment module for card-present and online transactions but this functionality is not in use.
INHERENT RISK	Low
AUDIT RISK	Low
RECOMMENDED PCI SERVICES	Self-Serve SAQ

Suggestions:

- The first step of the needs assessment is critical, so outsource and consult as much as required to ensure you identify and inventory everything properly. A misstep here could cost you significantly down the road.
- Make sure you capture more than just the maker of your POS devices. The model number is important and will be needed as part of your SAQ.
- Determine risk rankings and your risk tolerance. This is how you could summarize the findings of the needs assessment and prioritize remediation.
- Have strict institution-wide policies to keep all data safe.

Completing a needs assessment to kick off your PCI DSS compliance initiative can help provide some visibility into your efforts and give you some key data points to share with others. You will be able to identify merchants that are costing more to protect than they generate in revenue, find ways to reduce scope and technology risk, and use all this information to help develop an assessment strategy moving forward. This will give your PCI DSS compliance initiative some early wins in securing funding and executive buy-in to keep the initiative going.

Part Two: Grouping Your Merchants

Once you've gathered data on your university's merchants, there are a few ways you can go about ensuring their PCI DSS compliance. Before choosing a method, however, break your merchant list into more manageable pieces. After all, not every merchant functions exactly the same way—approaching them all en masse is not only more expensive but also a bigger headache. On the other hand, evaluating each merchant individually isn't an option for every university for several reasons. Group data collection prevents the overtaxing of resources—time, funds or workforce— required by collecting data on merchants separately, and you'll be collecting less data overall.

There are a few strategies you can use when putting your merchants into groups. You can divide by SAQ type, risk, payment acceptance or the requirements of your acquiring bank.

Based on SAQ Type

Different varieties of PCI SAQs are available, making this an excellent option for universities who have more than one type.

SAQ A

SAQ A is for "card-not-present" merchants, who outsource all cardholder data functions—that is, they only accept e-commerce, mail or telephone orders, and don't store (analyze or report on) cardholder data. These merchants are not required to do vulnerability scans or penetration tests.

SAQ A-EP

SAQ A-EP is for e-commerce only merchants who outsources all cardholder data functions to a PCI-DSS- validated third-party payment processor, including any payment pages. The e-commerce website does not hold, retain, or analyze any cardholder data, and only keeps paper receipts or reports. In addition, the e-commerce website is not connected to any other system in the environment. These merchants must do internal vulnerability scans, external vulnerability scans, and penetration testing.

SAQ B

SAQ B is for merchants with only imprint machines, or only stand-alone, dial-out terminals, who don't store electronic cardholder data. SAQ B-qualified merchants don't transmit data over any network (internal or external) and only retain paper reports or paper copies of receipts with cardholder data. Those documents are not received electronically. SAQ B also doesn't require vulnerability scanning or penetration testing.

SAQ B-IP

SAQ B-IP merchants only use standalone PTS-approved Point of Interaction (POI) devices connected to a payment processor via IP. Note, however, that POI devices must be approved on the PCI DSS website. All cardholder data is transmitted through these approved devices, and do not rely on any other device (e.g., computer, mobile phone, tablet, etc.). The only retained information, whether receipts or reports, are in paper form. There is no information stored electronically. SAQ B-IP merchants must perform external vulnerability scanning, but not internal vulnerability scanning or penetration testing.

SAQ C

SAQ C merchants have payment application systems connected to the Internet, but do not store cardholder data. The payment application/Internet device is not connected to any other systems in the merchant's environment (which can be effectively achieved through network segmentation). These merchants' LAN is for a single location only, and is not connected to any other locations. SAQ C merchants only retain paper reports or paper copies of receipts, and the payment applications use secure techniques to provide remote support to the payment system. Both vulnerability scans and penetration testing are required.

SAQ C-VT

SAQ C-VT merchants' only payment processing is done via an Internet browser, on web-based virtual terminals without electronic cardholder data storage. The terminal solution is provided and hosted by a PCI DSS-validated third-party service provider. Meanwhile, the merchant accesses the solution via a computer that is isolated in a single location, not connected to any other system within the environment or beyond. In addition, the computer does not have cardholder data storage software (such as batch processing or store and forward), and there is no hardware that captures cardholder data (like card readers). The merchant doesn't receive or transmit any cardholder data. No vulnerability scans or penetration tests are required.

SAQ D

SAQ D is the compliance requirement for merchants who do not meet the criteria for the other SAQs (A, B, C, C-VT, or P2PE-HW), and for other service providers who are deemed eligible to complete it. It's important to note that SAQ D is without a doubt the most comprehensive SAQ, as it includes provisions for all 12 of the PCI DSS requirements. Both vulnerability scans and penetration testing are required.

SAQ P2PE-HW

A point to point encryption (P2PE) solution is provided by a third-party solution provider, and is a combination of secure devices, applications and processes that encrypt data from the point of interaction (at the point of swipe or dip) until the data reaches the solution provider's secure decryption environment.

A P2PE solution must include the following:

1. Secure encryption of payment card data at the point of interaction (POI)
2. P2PE validated application(s) at the POI
3. Secure management of encryption and decryption devices
4. Management of the decryption environment and all decrypted account data
5. Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration and usage.

SAQ P2PE-HW questionnaires are for merchants only using hardware payment terminals included in a PCI SSC-listed, validated P2PE solution with no electronic cardholder data storage. SAQ P2PE merchants do not have access to clear text cardholder data on any computer system, and only enter account data via validated hardware payment terminals. The merchant must have implemented all controls in the P2PE Instructions Manual (PIM) provided by the P2PE solution provider. This SAQ does not require vulnerability scans or penetration tests.

Risk

Taking a risk-based approach to PCI DSS compliance is a great idea. To do this you want to treat each merchant individually and develop a risk profile for each. This is a complex process and might require third-party assistance.

Payment Acceptance

You can categorize your merchants by their payment method. Often times, this will separate merchants by size, risk, vulnerability and merchant level automatically. Extremely small vendors, for example, might accept cash only, while your bursar accepts a wider range of currency exchange.

Here are some examples categorized by payment acceptance channel:

- Card present
- Card not present (Mail Order/Telephone Order)
- Virtual Terminal
- E-commerce
- Point of Sale systems

Each method has its own set of security concerns, and separating your merchants using these parameters may help you move forward with your university's PCI DSS compliance.

Acquiring Bank

Your acquiring bank might specify for you what their expectation is for your SAQ filing. Every acquiring bank might require something different, adding a further layer of complexity to your PCI DSS compliance program. If you use multiple acquirers and they are requesting different things, schedule a meeting with them to discuss how you can meet their needs while not adding further complexities to your project. A simple call can help realign their expectations and/or clarify what they expect you to do.

Part Three: Building a PCI Team

Whether you're pursuing PCI DSS compliance for the first time or you've already started the process, you've probably realized by now that building a core team is critical. Each task is riddled with barriers and challenges; having an informed team allows you to resolve each issue more quickly and efficiently. Without a core PCI team, the project will likely lose momentum and could fall apart.

First, consider the responsibilities of a PCI DSS compliance core team: Who will ultimately sign off on your SAQ(s)? Who oversees merchant accounts but can also address the other business areas involved in PCI? Keep in mind that this is a business issue shared jointly between Finance, Treasury, and IT. The team member responsible for signing off on the SAQ(s) will need to have access to data about your organization's compliance status and any remediation that might be taking place.

To provide this high level of oversight you should build a PCI core team or working group comprised of key stakeholders from different business groups involved. Team members should have the authority to make changes to the environment as well as policies and procedures. The working group should also report up to a steering committee that manages multiple different compliance and/or security initiatives. The steering committee would then report to the board.

Once your team is built and you have decided who can sign off on your SAQs, you must determine if you have the skills in-house to self-validate your compliance or if you need help from a third party.

How do I know if I need third-party help?

PCI is a constantly evolving standard and keeping up to date with all of the requirements, auditing standards, and evidence validation can be a full job in itself. As a result, large universities might have several full-time staff members that work solely on PCI DSS compliance.

Universities with self-managed programs are further along in the process and have already laid the essential framework. Oftentimes, they have established policies and procedures and sent their staff to specialized PCI training. Programs can certify staff for PCI Professional (PCIP) or Internal Security Assessor (ISA), both provided by the PCI Security Standards Council. These schools also have internal auditors or security staff with certifications like the Certified Penetration Testing Engineer (CPTE), GIAC Security Essentials (GSEC), Certified Treasury Professional (CTP), and Certified Information Systems Security Professional (CISSP). No one person can possibly have all the available credentials or experience to manage the program from every angle on their own. Finally, schools that manage their own compliance internally typically have a Qualified Security Assessor (QSA) that they retain and consult with on a very limited basis as needed. Oftentimes, their team also relies on automated third-party tools to help track and manage their compliance programs.

On the other end of the spectrum there are other schools that prefer to use a third party to manage and evaluate their compliance annually, avoiding the commotion of creating a team altogether.

The school will contract a qualified, experienced QSA with its own team to support the school's compliance program. Schools that need to use a third party in depth:

1. Lack staff/manpower to complete an assessment
2. Have too wide a scope to be supported internally
3. Have complex environments that cannot be assessed internally due to lack of an experienced staff
4. Need the independence of having an outside firm assess them
5. Can benefit from the technical experience of a QSA firm
6. Are going through their first PCI compliance process and need support

If you decide to select a QSA, ensure that they have experience working with the technologies in your environment and can support you with more than just PCI if needed. Make sure the organization has the right methodology to get through an assessment of your size and scope and look for an Approved Scanning Vendor (ASV), Payment Application QSAs (PA-QSA), and Point to Point Encryption QSAs (P2PE-QSA). Availability of these services shows that the QSA is well rounded and has experience with a variety of technologies.

Part Four: Assessing Your Merchants

Once you've built your team, identified your merchants and grouped them into logical categories, you can begin your assessment phase. This is probably where your team or QSA will provide the most help.

Assessing the merchants is critical to staying compliant. Many merchants will buy into the myth that they are compliant because their payment processing vendor is compliant. Compliance is a combination of both the vendor and the merchant's environment. Therefore, if your campus has a merchant that accepts payment, you must validate them to meet PCI DSS requirements. Assessing vendor-by-vendor will likely be too big an undertaking, even by the average QSA's standards, so grouping them is advisable.

Once you've grouped merchants, determine each group's scope: What is actually in and out of scope? What questions are applicable and which ones are not? Which controls are being managed by a third party? Do you have an Attestation of Compliance (AOC) for the vendor you are using to manage some controls for you? Asking questions like these helps validate scope, simplifying the process of arranging meetings with stakeholders as well as the discussions you must have with them. You want to make sure you're asking the right person the right questions, otherwise you might have to go back with more questions because you left something out the first time.

PCI DSS compliance is a complicated process and requires multiple people to validate controls; for example, certain SAQ types may require meetings with four or five different people. The process also includes collecting and documenting evidence in the event that anything goes awry. At any point you should be able to go back to your work group and collect information from the audit, including: Who did you talk to during your last audit? Who is responsible for what controls? What evidence supports each requirement?

Compliance Management Tools

Most schools leverage a compliance platform that documents the assessment and manages the archives in one convenient place. Such platforms can provide the steering committee, executive sponsor, and signer oversight of the PCI DSS compliance program they need to make important decisions around compliance.

Moreover, since so many people are involved and a variety of information needs to be collected, it is helpful to have one central repository that stores all your PCI DSS related information. A compliance management tool allows team members to work independently of one another on the SAQ(s) and/or merchants while performing the assessment. There's also a much lower likelihood of losing information when transitioning from one member to another. Communication gaps are all too common.

First Time Assessing Your Compliance?

First-time assessments can be overwhelming. If you find that your project is just too much to handle, don't panic! Yes, PCI DSS compliance is a challenge and it will take a significant amount of time and effort to comply. Set the expectations of your possible outcomes and your organization's internal time line early. The length of time your project needs will vary based on the size, complexity, resources, and buy-in you have. Regardless, it is unlikely that you will be 100% compliant the first time through an assessment. It is not uncommon to find gaps that need to be remediated afterward.

If you think you need to remediate your organization's findings you should work with a third-party QSA to help determine appropriate remediation and develop a prioritized remediation plan. You can download the PCI Data Security Council's prioritized remediation template at: https://www.pcisecuritystandards.org/documents/Prioritized_Approach_v3-1.xlsx