How to Develop a PCI Compliance Program

And Take a Step on the IG Career Path

Andrew Altepeter

Any organization that processes customer payment cards must comply with the Payment Card Industry's Data Security Standard or face possible fines and a great potential for this sensitive information to be compromised. Leading the PCI compliance program's development is a prudent way for a RIM professional to raise awareness of information governance (IG) priorities and, perhaps, take a step toward a broader IG career.

Information governance (IG) and records and information management (RIM) professionals will readily agree that protecting sensitive information is a top job priority and that it has become more difficult and risky because of the explosion of electronic information. Its importance has been underscored by privacy legislation, such as the Fair and Accurate Credit Transactions Act (FACTA), the Health Insurance Portability and Accountability Act (HIPAA), and European Union privacy directives.

As seen by the constant media stories about data breaches and their negative impact on even the most established and respected merchants, handling sensitive information properly is necessary not only to meet business and customer needs, but to prevent severe business disruptions, damaged customer relations, and negative public perceptions that can occur when it is compromised.

ARMA International recognized this important priority in creating the Principle of Protection as one of its eight Generally Accepted Recordkeeping Principles® (Principles). It codified this principle as the need to "ensure a reasonable level of protection for records and information that are private, confidential, privileged, secret, classified, or essential to business continuity."

This emphasizes the imperative for RIM professionals to be involved in the creation and maintenance of policies, processes, and procedures that protect sensitive information. As a bonus, building a compliance program of this type provides an opportunity to expand their skills beyond traditional RIM roles and advance along an IG career path.

PCI DSS: Mitigating the Risk

For organizations that process customer payment cards (either debit or credit), this is one of their most critical types of information to protect, and the risks surrounding it have grown steadily over the last few decades because of the growing use of e-commerce and volume of electronic payment processing.

In 2003, the U.S government responded by passing FACTA, which includes requirements for free annual credit reports, fraud alerts, truncation of payment card numbers, and certain protections for victims of identity theft. However, it lacks specific measures for organizations to strengthen security and prevent breaches.

In 2006, the major payment card companies (Visa, MasterCard, American Express, Discover, and JCB, which is a Japan-based payment card allied with Discover in the United States) formed the Payment Card Industry Security Standards Council (PCI SSC), with requirements for *merchants* – which it defines as "any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC."

The primary objective of this organization has been the production and maintenance of the Payment Card Industry Data Security Standard (PCI DSS), which has given all merchants who process payment cards common controls to help reduce exposure to fraud. There are six goals, which are further broken down into 12 requirements as shown in Table One below.

A cursory look at the requirements demonstrates the interdisciplinary approach organizations must take to reach PCI compliance. Input will be needed from finance, IT, information security, and information governance teams. Executive sponsorship is re-

Payment Card Industry Data Security Standard

Goals	Requirements
Build and maintain a secure network.	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system pass.
Protect cardholder data.	3. Protect stored cardholder data. 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. 6. Develop and maintain secure systems and applications.
Implement strong access control measures.	7. Restrict access to cardholder data by business need-to-know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly monitor and test networks.	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an information security policy.	12. Maintain a policy that addresses information security for employees and contractors.

Table 1: PCI Requirements

quired, especially from finance and the business units processing payment cards.

Complying with PCI DSS should be a top priority for all merchants, as failure to comply could result in fines from the payment card companies and banks. In addition, states such as Minnesota, Nevada, and Washington have passed laws that require all merchants who do business in their state to be PCI compliant.

Developing a PCI Compliance Program

While achieving compliance may seem a tall task, IG professionals should view this challenge as an opportunity: implementing a PCI program gives them an excellent opportunity to expand the scope of their job duties, provide meaningful value to the business, and increase their visibility. Here are some steps to getting started:

1. Build Expertise

The PCI DSS makes all of its resources for its requirements and standards available at *www.pcisecuritystandards.org*. Take some time to read through the requirements, documentation, and available training. Enroll in PCI awareness training or Payment Card Information Professional credential training, both available through the PCI Security Standards website.

2. Form a Team

Running a successful PCI compliance program requires a multidisciplinary team, including people from the following departments.

Finance. The team will need executive sponsorship from finance, as a CFO or equivalent executive officer will need to sign an Attestation of Compliance for the organization's receiving bank. Finance should also assist in creating training and operating procedures for employees processing credit cards.

IT. Someone will need to be able to speak to the organization's network architecture, firewalls, antivirus software, and desktop image. In addition, new software may need to be purchased, and IT policies may need to be updated.

Information Security, Legal, or Privacy. Some assistance from legal or data privacy may be needed, and depending on their place within IT, additional representatives from information security may be needed. Relevant policies should be updated, and these resources may be required to implement some of the PCI requirements.

Internal Audit. While optional, leveraging internal audit resources to effectively monitor and enforce PCI controls reduces the burden on RIM and gives the compliance program added enforcement.

Records and Information Management. See the section "RIM Professional Roles" toward the end of this article.

3. Scope the Cardholder Environment

Work with team members to determine the scope of the card environment. This includes anywhere within the organization's infrastructure that payment card data is stored or transmitted. Payment card data includes the primary account number, cardholder name, service code, expiration data, full magnetic stripe data, three-digit code on the back of the card, and PIN.

The scope may include both electronic and paper information, computers, networks, and finance applications. Completing a network diagram, one of the PCI requirements, will be

helpful in determining scope. Make sure to have an updated roster of anyone who comes in contact with payment card information. Find out from finance the annual number of payment card transactions and how many dollars the organization processes.

4. Determine Requirements

While PCI DSS applies to all organizations that take payment cards, requirements are applied differently, depending on the type of merchant. These levels are determined by the merchant's annual number of payment card transactions. Each payment card company defines its merchant levels slightly differently. For example, Table 2 shows the merchant levels Visa defines.

Merchant Level	Annual Number of Transactions
Level 1 Merchant	6 million or more
Level 2 Merchant	Between 1 million and 6 million
Level 3 Merchant	Between 20,000 and 1 million
Level 4 Merchant	Less than 20,000

Table 2: VISA Merchant Levels

An organization's compliance is tracked by its acquiring bank, which is the financial institution that processes credit and debit card payments for products and services. Major banks have teams that are happy to assist merchants with PCI compliance. They can be contacted through the bank's merchant services division.

An organization's level has a significant impact on what compliance activities it is required to complete. For example, large merchants are required to have either a qualified security assessor or internal security assessor evaluate their environment for PCI compliance, and they must have quarterly vulnerability scans by an approved scanning vendor.

Smaller merchants are able to complete a self-assessment questionnaire (SAQ) and submit it to their acquiring bank. There are also several variations of SAQ; the one that is most appropriate for the methods the organization uses to process payment card information should be chosen. PCI SSC recognizes that the requirements may seem overwhelming to small businesses. See *www.pcisecuritystandards.org/smb/* for a helpful guide for helping small merchants comply with the requirements.

5. Work to Reduce Scope

Certain steps make complying with PCI DSS much easier. Using firewall software, segment the card environment from the rest of the network. Do not store payment card data within the organization's environment. Outsource card processing to a payment application that has been validated by a Payment Application Qualified Security Assessor. (See a list of validated payment applications at *www.pcisecuritystandards.org/approved_companies_providers/*.)

If possible, use *tokenization* – which replaces payment card data with a numeric signifier – to completely eliminate all payment card information from applications. The payment card information is stored with a PCI-compliant provider, with only the token visible to the merchant. Many validated payment vendors offer this service.

6. Establish and Maintain Compliance

It may take time to implement a PCI compliance program. A seasoned project manager may be needed to bring together team members from disparate departments. But do not lose heart: once established, the organization will be more secure, avoiding embarrassing breaches and loss of customer trust.

Reaching compliance is not the end of the road, though; remaining compliant requires an ongoing effort. Employees must continually be

trained and the environment must stay compliant through hardware and software upgrades. The organization must certify compliance annually, and many requirements must be satisfied on quarterly or biannual cycles.

And let's not forget: business happens, and that means ever-changing scope, hardware, and software. Make sure all members of the PCI team continue to meet monthly or quarterly to track the scope and compliance of the entire environment.

The RIM Professional's Role

Even if they do not become PCI compliance program leads, RIM professionals should provide inputs and be part of the team. RIM participation is essential in the following area.

Scoping the Payment Card Environment

The very first step in setting up a PCI compliance program is scoping the environment to determine what system components are subject to the PCI DSS. Because the RIM function has the duty of managing information enterprise-wide, it has a unique ability to locate the repositories where customer payment card data may reside. This includes order processing applications and databases, receipts, backup tapes, and any number of other records on both electronic and paper media.

Analyzing Data Flows, Business Processes

RIM professionals are in a unique position to see the big picture. They can see how data flows through seemingly disparate processes and repositories. After scoping the payment card environment, a RIM professional may be able to assist finance and IT in improving business processes for better efficiency and security.

Assessing Vendors

The PCI DSS requires merchants to track the PCI compliance of their suppliers and vendors. The organization's vendor security questionnaire should include a least one question on that vendor's PCI compliance. This is especially crucial if managing vendors for offsite records or data backup, which could potentially include the storage of customer card data. Make sure to investigate vendors' PCI compliance status before signing a contract, and track their compliance on at least an annual basis.

Updating Policy

While the organization may deem it necessary to create a separate policy regarding PCI compliance, any RIM or information security policies should include references and requirements to compliance with the PCI DSS. Incorporating these requirements into existing policies ensures all relevant team members are aware of the requirements and their responsibilities.

Adding Value, Developing an IG Career

Whether a member of a PCI compliance team or in a leadership role and a PCI subject matter expert, a RIM professional's involvement will add demonstrable value to the organization. The organization will value the efforts made to make the cardholder environment more secure, improve customer trust, and minimize the risk of noncompliance with bank regulations and state law, and the associated fines that may result.

Perhaps most importantly, taking the lead in a PCI compliance program is a prudent way to expand a career path from one narrowly defined in RIM to a more comprehensive IG career. It will also allow a RIM professional to develop relationships with other parts of the organization and expand the presence and awareness of IG priorities. **END**

Andrew Altepeter can be contacted at andrew.altepeter@gmail.com. *See his bio on page 47.*