


Using GRC for PCI DSS Compliance

GRC Spotlight

powered by LockPath®



HARLAND CLARKE®

A person wearing a blue hoodie is shown in profile, focused on typing on a laptop. The scene is dimly lit with a strong blue color cast, suggesting a nighttime or low-light environment. The person's hands are positioned over the keyboard, and the laptop screen is partially visible on the left side of the frame.

The ongoing struggle to protect sensitive credit card data will continue to **escalate**. Increasingly sophisticated attacks have targeted financial institutions of all sizes, infiltrated retailers, and foisted multiple strains of malware on many unsuspecting targets.

Data breaches involving personal information, such as credit card data, can cost a financial institution its reputation, future revenue and the expense of restitution.



Each security standard has several layers of sub-requirements, with more than **200** in all.

One of the requirements used to tackle this problem is the Payment Card Industry Data Security Standard (PCI DSS).

It provides a uniform set of data security requirements to govern all organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM and point-of-sale (POS) cards. These standards are enforced and updated by the Payment Card Industry Security Standards Council, founded and governed collectively by the major credit card companies.

The standard applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers and service providers. It also applies to all entities like financial institutions that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

The Requirements of PCI DSS

PCI DSS consists of 12 requirements in six categories that include:

- 1 Building and maintaining a secure network and systems
- 2 Protecting cardholder data
- 3 Maintaining a vulnerability management program

- 4 Implementing strong access control measures
- 5 Monitoring and testing networks
- 6 Maintaining an information security policy

The 12 requirements cover everything from installing appropriate firewalls and protecting all systems against malware to restricting physical access to cardholder data. The requirements can be roughly subdivided into two groups: policies and practices.

Policies are generally self-evident. For example, Requirement 12 states, “Maintain a policy that addresses information security for all personnel.” *Practices* tend to mandate explicit security solutions. For example, Requirement 8.3 states the requirement to “Incorporate two-factor authentication for remote access ... to the network by employees, administrators, and third parties.” Almost all practice requirements have an implicit policy requirement.

Each standard has several layers of sub-requirements, with more than 200 in all. For example, Requirement 3 — protecting stored cardholder data — consists of seven subsections. Subsection 3.6 has eight requirements.

The PCI DSS Hierarchy

At the top of the heap are the card brands that maintain the PCI DSS system. Next down are the acquirers like financial institutions that act as intermediaries between the brands and the merchants. Last are the merchants, who initiate transactions at the behest of customers, through acquirers to the brands.

There are up to four levels of merchants. Level 1 merchants are the largest and Level 4 merchants are the smallest, by number of annual transactions per brand. Each card brand maintains its own system for determining merchant level, and may not have four levels. In general, the level determines the extent of attestation requirements that must be met annually.

One additional player may also be involved: the processors. Processors serve as an additional middleman in transactions, providing added value such as aggregating payment card types. For example, American Express® and Discover® Card are traditionally “closed” systems, and thus are not necessarily packaged by acquirers.

The card brands are ultimately responsible for enforcing their respective security programs. The PCI Council, which maintains PCI DSS and related standards, does not have any enforcement authority. The standard is referenced by each card brand’s security program, but the contractual relationship is generally between the brands and the acquirers, and in turn, between the acquirers and the merchants. In the event of a cardholder data breach, the card brands will

assess a fee on the acquirer, which will in turn assess an additional fee on the merchant. There is rarely a direct interaction between card brands and merchants.

From the brands’ perspective, merchants are as much a part of the threat community as hackers. As such, merchants should understand that PCI DSS does not exist directly for their own benefit and protection, but rather as a risk management treatment (remediation action) initiated by the card brands. Merchants should account for this perspective when incorporating PCI DSS requirements into their own risk management programs. Maintaining the wrong perspective could have a detrimental impact. It is also worth noting that several U.S. states have adopted part or all of PCI DSS as law.



The Challenge of Compliance

Each PCI DSS requirement contains an exhaustive list of testing procedures to ensure compliance. Financial institutions must validate their compliance annually. Two options are available based on transaction volume:

- Those with a large volume of transactions can use an external Qualified Security Assessor (QSA) designated by the PCI Council to create a Report on Compliance (ROC).
- Those handling a smaller volume can use a Self-Assessment Questionnaire (SAQ).

Officials with the PCI Council have publicly acknowledged the challenge of implementing and maintaining PCI DSS, especially in light of increasingly complex business and technology environments. Many financial institutions only partially comply with the standards.

The latest update to PCI DSS made compliance even more demanding. Financial institutions are now responsible for reviewing a third party's procedures for handling your customer's PCI data. All third parties must acknowledge they are compliant, in writing.

The Failed One-Off Approach

Historically, one of the biggest problems with PCI DSS compliance initiatives is treating the standard as a unique and independent set of requirements instead of integrating the requirements into a holistic program. This one-off approach neglects the reality that PCI DSS is part of the financial institution's risk management program, leading to poor scoping of efforts and, in the end, data breaches.

When PCI DSS was first released, most organizations immediately shifted to an approach that had been used for compliance with the Sarbanes-Oxley Act of 2002 (SOX). This meant limiting audits and security efforts to only those systems and applications that were directly in-scope, without providing meaningful security improvements across the entire enterprise. Unfortunately, whereas data contained within "financially significant systems" (as impacted by SOX) may or may not have held much value for outside attackers, systems accepting and processing credit cards for payments absolutely held intrinsic value. As such, attacks on these systems have increased significantly over the past 10+ years, often exposing weaknesses in this one-off security approach.

This one-off approach is most noted by the holes it leaves in an organization's overall defenses. Systems and applications considered in-scope for handling cardholder data are often relatively well secured, but surrounding systems are typically less fortified. In practice, this leads hackers, who operate on efficiency principles, to attack the weakest links — internal, non-PCI DSS systems — to gain access to the more tightly controlled cardholder environment without having to defeat it head-on. In many cases this attack approach is even more challenging to detect because access is often expected and allowed.

The failure in this approach is focusing too heavily on securing the cardholder environment and not investing adequate efforts into securing the rest of the computing environment. Moreover, PCI DSS is particularly prescriptive, causing organizations to invest heavily in specific areas without extending key functionality to the rest of the enterprise. This failure is magnified by inadequate extension of monitoring and response capabilities, which are particularly important in reducing the negative impact of a data breach. Organizations should manage their own risks and meet PCI DSS requirements through an integrated, holistic approach to enterprise security.

The one-off approach is most noted by the holes it leaves in an organization's overall defenses. It leads hackers, who operate on efficiency principles, to attack the weakest links.

An effective GRC program helps financial institutions automate their business processes, reduce their enterprise risk and demonstrate regulatory compliance.

The GRC Approach to PCI DSS

Financial institutions can simplify the process by incorporating PCI DSS into their business-as-usual systems rather than treating PCI DSS as an isolated problem with a separate solution. Complying with PCI DSS should be a core element of a holistic approach to your overall governance, risk and compliance (GRC) program.

An effective GRC program helps financial institutions automate their business processes, reduce their enterprise risk and demonstrate regulatory compliance. A GRC program provides coordinated control over these activities to help a financial institution operate more efficiently. When these tasks are managed independently from one another, organizations will have substantial duplication of tasks. A disconnected GRC approach is like a poorly planned transport system in which individual routes operate, but the entire network does not work effectively together.

Having a solid GRC program allows you to properly frame and address responsibilities without creating a one-off scenario. Such a program allows organizations to manage their own risk rather than having a risk management approach dictated to them.

GRC Spotlight:

Aligning PCI DSS Requirements with Your Risk Management

As a leading GRC platform, Harland Clarke's GRC Spotlight, powered by LockPath, provides several capabilities that enable financial institutions to set up and manage an effective and unobtrusive GRC program that aligns PCI requirements with their own risk management programs.

Policies & Controls

Rather than building your GRC program to fit PCI DSS, build it to match the needs of your entire organization. To that end, the GRC Spotlight policy and controls framework provides a common starting point for defining and articulating the structure and details of that program. The Compliance Manager app provides key capabilities that support this approach.

If your organization has an existing set of policies and controls, the first step is to enable and configure that set directly within Compliance Manager. If that set does not exist, then the approach may vary. For example, if policies do not exist, template policies associated with those activated controls and authority documents can be used.

The next step is to iterate through the controls, customizing them to your environment. GRC Spotlight maintains an auditable history of changes made in both controls and policy documents. The scoping activities should be conducted in a manner that tailor both frameworks to your specific environment, rather than simply trying to adopt PCI DSS requirements without evaluating their appropriateness. Part of the iterative scoping and editing process should include a risk analysis step that helps weigh the impact of a given control or policy on the business.

Compliance Manager is specifically designed to ease the burden of developing policy and control frameworks, as well as to expedite the integration of additional requirements. Furthermore, Compliance Manager can be used to conduct awareness events for users — which helps to meet security awareness requirements — and to conduct security assessments.

Mandated Practices

PCI DSS is considered a prescriptive standard, which means it articulates specific technical measures that must be implemented in order to achieve full compliance. Although GRC Spotlight does not directly implement these measures, it does provide a ready capability for documenting requirements, issuing awareness events to affected internal teams, and conducting routine assessments to ensure that the practices are being implemented as required.

Documentation of controls and policies can be performed within the Compliance Manager app, which can also be used to conduct assessments to measure conformance with requirements. Vulnerability scan data can be imported within GRC Spotlight's Security Manager app to help monitor the state of compliance with key directives. And, the Incident Manager and Risk Manager apps can be used to capture deficiencies in practices, as well as to actively manage remediation activities.

Risk Management

A goal for your financial institution may be to develop and manage your own risk profile, rather than use one from another organization. To that end, the Risk Manager app can be used to identify, assess and manage treatment of risk areas. Risk Manager also provides the ability to track exceptions and follow up on associated remediation activities. The app can be used alone or in conjunction with other GRC Spotlight products to correlate risk items with other content.

The availability of the platform's patented Dynamic Content Framework (DCF)¹ tables within Risk Manager provides the means to create additional sets of records for managing unique aspects of the risk management program. For example, it may be useful to break out risk areas that correspond directly to PCI DSS compliance efforts to more efficiently track and report on status. This is of particular value when tracking remediation activities in an effort to minimize fines due to non-compliance.

Testing

In an ideal world, all testing could be automated with minimal need for manual input or intervention. However, that time has not yet arrived, which means there is a need for optimizing manual testing activities. GRC Spotlight can help manage the testing burden in two key areas.

First, the Security Manager app can be used to track vulnerability scan results. These scans are typically performed on at least a quarterly basis, and remediation of findings must be completed in a reasonable period of time to allow for a re-scan that produces a result of "passed."

Vulnerability scan data can be combined with asset information within the Security Manager app to help provide a more complete device security history. Additionally, the Incident Manager app can be used to document deficiencies and track remediation status. Security Manager also supports DCF tables, which can be custom-built to support other technical testing activities as well.

Second, GRC Spotlight — via the Security Manager, Risk Manager, Incident Manager and Compliance

Manager apps — can be used to conduct continuous monitoring and testing to ensure that the organization not only reaches compliance once a year, but that compliance is in fact maintained in a reasonably high state year-round. Moreover, the Vendor Manager app can be used to assess third parties as part of the overall GRC program to ensure that any risks represented by these external entities are properly tracked and managed.

Validation

Validation requirements vary depending on the merchant level. As noted earlier, Level 1 merchants are required to complete an ROC reflecting the results of the on-site assessment, as well as to submit an Attestation of Compliance (AOC) and the last four quarterly vulnerability scans, all with passing scores. For non-Level 1 Merchants, a SAQ may be sufficient, along with the AOC and vulnerability scan reports.

Of the three main reports required by PCI DSS, the ROC is the most onerous to complete. It must follow a specific format and include answers to each of the more than 200 testing procedures. Although it is desirable to automatically generate a ROC, there is not a convenient way to do so today. Instead, key aspects of the ROC can be collected through various techniques — via assessments within Compliance Manager, for example — and then exported from GRC Spotlight and integrated into a properly formatted report.

Both the AOC and SAQ are easily completed outside of the platform. Nonetheless, by integrating the policies and controls frameworks within Compliance Manager, most of the AOC and SAQ can be generated within GRC Spotlight and then exported for integration into the final document.

¹ United States Patent and Trademark Office Patent Number 8,874,621, "Dynamic Content Systems and Methods," 2014

A Coordinated GRC Solution

A one-off approach to PCI DSS compliance often results in increased risk factors by creating discrepancies in security levels between environments within the shared network. Such an approach can be overcome by focusing on a central GRC program that is designed to manage your organization's own risk profile, rather than the risk profile of the card brands.

GRC Spotlight can help you implement a coordinated GRC program for compliance with not only PCI DSS, but also with other rules, regulations, laws and certifications. Using GRC Spotlight, financial institutions can automate business processes and demonstrate regulatory compliance while reducing enterprise and IT risk. With our PCI solution, you can:

- Implement a flexible PCI DSS framework with the ability to map authority document citations and controls to your policies and procedures.
- Perform gap analyses on policies and procedures to assess your PCI compliance maturity level.
- Maintain a reportable asset profile of vulnerabilities, risks, incidents, events, controls and policies.
- Track incidents and streamline the processes of managing incident identification and remediation tasks.
- Assess third parties for compliance and report on findings.

Don't wait for a credit card data breach to take action. To request a live demo of our PCI DSS solution and discover how a holistic approach to GRC will better enable your organization to comply with PCI DSS, contact Harland Clarke.

Call 1.800.351.3843

Visit harlandclarke.com/GRC

Email contactHC@harlandclarke.com

About Harland Clarke

Harland Clarke is a leading provider of best-in-class integrated payment solutions, marketing services, and retail products. It provides integrated solutions for financial institutions; investment firms; business-to-business clients; individual consumers; and small, medium and large businesses serving multiple industries. Harland Clarke's clients range in size from major financial institutions and corporate brands to small businesses and individual consumers. Harland Clarke provides products and services to nearly 15,000 financial and commercial clients. harlandclarke.com