To improve PCI compliance, determine where your cardholder data is and monitor where it’s going.

On October 28, 2010, the PCI Security Standards Council (PCI SSC) released version 2.0 of the PCI DSS (Payment Card Industry Data Security Standard). v2.0 did not change the mandate; the DSS remains a standard assessment tool to help merchants, retailers and other entities that store, process or transmit cardholder data understand the controls and processes that must be in place to protect that data. But it did clarify “that the first step of a PCI DSS review is to accurately determine the scope of the assessment, by identifying all locations and flows of cardholder data and ensuring that all such locations are included in the assessment.” In other words, according to the PCI SSC, PCI compliance work should start with a determination of where cardholder data is and the ability to track where it goes. Without that, it would be hard, if not impossible, for an entity to be in compliance.

The reality is that 71% of companies that fail PCI audits do so because they cannot adequately meet Requirement 10, “Track and monitor all access to network resources and cardholder data.” And not being compliant poses a real security risk, 96% of breach victims subject to PCI-DSS had not achieved compliance according to the 2012 Verizon Data Breach Investigations Report. Companies that don’t know where all of their cardholder data lives can find themselves failing an audit when unencrypted spreadsheets, flat files and unprotected data stores in repositories like SharePoint are discovered during the assessment process.

And failing PCI is not cheap. If an entity fails, they must repeat the audit at an average cost of $225,000 US for a tier/level 1 merchant or retailer. The cost of failure doesn’t stop there. For example, payments service provider WorldPay indicates on their site that there will be a monthly $25k fee from Visa and a one-time fee of $25k from Mastercard assessed against non-compliant entities. Acquiring banks can increase transaction fees, raising the cost of failure even higher.

There’s a better way to deal with the PCI problem that combines both information and people centric approaches. It starts with knowing where the cardholder data is, and it wraps automated monitoring of data flows and a policy based approach around that data.
Five Things You Can Do to Improve Your PCI Compliance Posture

Here are the five things you can do to improve the process and increase your chances of passing the assessment.

1. **Get Scope under Control** - *Information Centric*
   As noted earlier, getting scope under control was deemed so important by the PCI SSC that a special section on the topic was added to v2.0 of the DSS to "to clarify that the first step of a PCI DSS review is to accurately determine the scope of the assessment, by identifying all locations and flows of cardholder data and ensuring that all such locations are included in the assessment." Anywhere cardholder data resides is considered "in scope" of the assessment, so finding that data and restricting it to a properly zoned CDE (cardholder data environment) is the most important step organizations can take.

2. **Monitor Traffic in Real-time to Identify Broken Business Processes** - *Information Centric*
   Once you know where the data is, you need to monitor where it’s going and who is using it. If the data flows outside of the CDE to another part of the organization or is accessed by a user that is not authorized to view it, the scope of the PCI assessment zone is increased. Many companies have business processes that pre-date PCI and include things like emailing a spreadsheet of cardholder data to another employee, business unit or outside of the company to external partners and assessors. Monitoring those flows and behaviors will help identify those processes so they can be addressed.

3. **Establish a Repeatable Process for Assessments** - *People and Process Centric*
   It’s inefficient if administrators need to scramble to gather the correct information, whether it’s
4. **Establish a Process to Mitigate PCI Risk - People Centric**

Business processes change, new systems are introduced, and new payment applications are implemented or updated on an ongoing basis at most companies. As changes occur - for example, new risks are discovered and old ones uncovered - an organization needs to have a plan for addressing those changes. And to be effective, this plan needs to incorporate all of the key stakeholders in a collaborative way. A risk framework and methodology that engages both IT and the business will result in a program that is adopted and supported by all user groups. When risk teams implement controls or processes without the support of the business it is common for users to look for ways to “get around” the process or control.

5. **Enforcement Containment of Cardholder Data - Information and People Centric**

Documented processes and procedures are a must for PCI compliance, but they won’t prevent all cardholder data from being leaked. A comprehensive PCI program needs technical controls to enforce the policy and prevent data from going where it shouldn’t or from being accessed by unauthorized users who do not have a “need to know.” Automating these controls where possible can increase security and reduce the burden on users. Consider a solution that detects credit card numbers in outbound mail and automatically enforces encryption of the data to protect it in transit. Or automatically flags the outbound message and holds it in quarantine until an appropriate party can manually review the message and approve or block the send in accordance with corporate compliance and business requirements.

**Practical Guide for Establishing PCI Improvement**

Now that we have laid out, at a high-level, the five steps for improving the PCI process, we’ll take a deeper dive into each area to discuss practical guidelines companies can use to put those steps into action.

**Getting Scope Under Control**

Since the first step towards PCI compliance is defining scope by ensuring cardholder data is restricted to the CDE, an organization needs a way to discover that data in an accurate and comprehensive manner. Discovering cardholder data through manual review of data stores is not feasible for most companies. To be truly effective, an organization will need to use an automated tool.

Key considerations for tool selection include:

- **Accuracy** - Valid credit card numbers from the five major card brands are fairly easy to recognize. They are 16 digits in length and adhere to ANSI standards. But not all 16 digit numbers are credit card numbers. To decrease false positives, the discovery tool needs to be able to identify which numbers are valid credit card data. The tool should have the ability to recognize card numbers according to the ANSI standards and increase accuracy with other checks such as the proximity of the number to other data and use of checksums, like the Luhn algorithm. PCI also states that certain information such as full magnetic stripe and CVV/CVC codes cannot be stored. CVC and CVV codes are three or four digits numbers that are hard to distinguish from other non-sensitive numbers. A tool that is able to assess proximity to other values may be used to accurately discriminate between stored authentication data and other non-sensitive data; this allows the organization to remediate the problem in advance of an assessment.
• **Scalability** - The explosion of cheap data storage means that even smaller companies may need to scan terabytes or petabytes of data to ensure that all places where cardholder data may be stored have been scanned. Look for a solution that can scan all of the data stores in your enterprise. This includes local hard drives on user machines and all of the servers in the data center. Another consideration is how quickly the scan can be accomplished, especially on large data stores.

• **Coverage Breadth** - If the only place credit card data is stored is an easily searchable RDBMs, discovery would be easier. The reality is that cardholder data is stored in a number of structured and unstructured locations including in emails, on email servers and in email attachments, in SharePoint and other collaboration repositories, in synchronized cloud repositories and in log files, notes or voice recordings from call centers. Credit card data is also found in Windows file shares, on Unix file servers, desktops, laptops, smartphones and tablets. Not to mention the variety of file types card data can be stored in including .txt, .docx, .pptx, .xlsx, .pdf, .ics, HTML and XML formats. An effective tool needs to be able to discover cardholder data in all these places and in all those formats. And with all these repositories and file types, it is important to have a solution that can distribute the discovery and monitoring load across multiple systems, locations and architectures.

• **Minimum Impact** - A corollary to the scalability consideration is how much the discovery tool will impact your business or performance for the end user. A comprehensive tool that brings the network to a halt and prevents customers from making purchases because the database is under load isn’t a good choice. Look for solutions that can be configured to do scanning during off hours or use low impact techniques like agentless scanning to minimize business impact.

### Monitoring Traffic in Real-Time to Identify Broken Business Processes

Once you know where the card data is and can take steps to ensure that the cardholder data is stored exclusively in the CDE, you need to make sure that the data isn’t leaving the CDE because of broken business processes.

• **Accuracy** - The points raised about accuracy in the preceding section apply here too. The monitoring tool must be able to discriminate between 16 digit numbers that are credit card and other 16 digit numbers to reduce false positives.

• **Flexibility** - Resources in most IT departments are scarce and tracking down every broken business process might not be cost-effective. Although no unauthorized, unprotected transmission of a credit card number is appropriate for compliance, there is a different risk level associated with a process that exports one credit card number per month versus one that exports thousands of credit card numbers in an unprotected spreadsheet out of the CDE every day. To ensure the IT team is focusing resources effectively look for solutions that can be tuned for specific business risk criteria like number of card numbers in a document or to focus monitoring on a higher risk business unit.

• **Non-Intrusive** - The idea of blocking an activity that could put the organization at risk is appealing but in practice pro-active blocking would be easier. The reality is that cardholder data is stored in a number of structured and unstructured locations including in emails, on email servers and in email attachments, in SharePoint and other collaboration repositories, in synchronized cloud repositories and in log files, notes or voice recordings from call centers. Credit card data is also found in Windows file shares, on Unix file servers, desktops, laptops, smartphones and tablets. Not to mention the variety of file types card data can be stored in including .txt, .docx, .pptx, .xlsx, .pdf, .ics, HTML and XML formats. An effective tool needs to be able to discover cardholder data in all these places and in all those formats. And with all these repositories and file types, it is important to have a solution that can distribute the discovery and monitoring load across multiple systems, locations and architectures.

### Data loss prevention solutions helped Microsoft discover sensitive data for PCI and other compliance initiatives.

- 12TB of data
- 30,000 file shares
- 120,000 SharePoint sites

“Before we could do anything, we knew we had to locate our sensitive information and measure compliance to the policies already in place,” Olav Opedal, Security Program Manager at Microsoft.

To execute their strategy, Microsoft needed a way to scan any managed space where sensitive data could be stored. This was a content-discovery challenge.

“The unparalleled accuracy and unique features of RSA DLP Datacenter made it the only viable choice for discovering all our sensitive content.”
Practical Guide to Improving PCI Compliance

can bring a critical system down and impact the business bottom line. Loss of customers may be more impactful than loss of some data. A monitoring solution should be able to focus on the detection and alerting of an activity first and blocking if and only if the company deems that is the appropriate action. Another option is a solution that can do a partial block, such as a temporary quarantine on the data while an administrator is alerted and can decide which permanent action to take.

- **Alerting** - Though this is last in the list, it is by no means the least important consideration. For example, can alerts be sent to the right person and is there a method for tracking response to the alert so that if the issue is not addressed according to corporate incident handling timeframes, subsequent alerts can be sent and an escalation procedure can be followed? How much information do the alerts have? Is the location of the file or data in question included and, if there is an owner, is that part of the alert? Ownership can be a critical piece of data because it indicates who should be contacted if a file or dataset is being used in a manner inconsistent with policy. Another consideration is whether or not the alerts can be used as part of an end-user education program. For example, if a user attempts to send card data out of the organization without proper protection, the system not only blocks the send but also communicates back to the sender via an alert that explains why the message is being blocked and what the sender can do, such as encrypting the file, in order to be able to send it out of the organization in a PCI compliant manner.

**Establishing a Repeatable Process for Assessment**

Knowing which information you need and continuously gathering it in the months leading up to an assessment will shorten the preparation time needed for the assessment and increase the likelihood that all the information the assessor needs will be available. To be effective, documented procedures need to in place augmented by tools that can gather and report on the relevant information. Many organizations use GRC tools to manage and monitor this process and provide process efficiency through customizable vendor supplied reporting templates and control automation. However, some organizations use their own homegrown tools or even spreadsheets for assessment management and oversight. Whichever approach an organization uses, it should have, at least, the following characteristics.

- **Tracking Progress** - Prior to the PCI assessment, an organization should review the entirety of v2.0 that contains the checks that the assessor will use. The DSS spells out exactly which controls and processes must be in place for compliance and can be used by any organization as an assessment tool in advance of an assessment to prepare the organization. As the company gathers this information, they can use the tracking tool to help manage progress and assess readiness level. For example a company can check all the required documentation into a repository and create a ticket for documents that are out of date, not in compliance with PCI, or nonexistent so they can be completed prior to the assessment.

- **Centralized Management** - The core purpose of PCI is to ensure that cardholder data is properly protected. Requirement 7 talks to access of that data: “Restrict access to cardholder data by business need to know.” Keeping a record of where data goes and who has access to it is a critical component to meeting this requirement. And placing access control policies on who can see and change that data is as important. Having a tool that can centralize the management of this process and extend policies to all documents and systems with cardholder data will help normalize compliance and provide a detailed assessment trail of the PCI related activities. Controlling access based on roles, with a special “business need to know” role or set of roles is another way to use centralized management to foster the repeatable assessment process.

- **Historical Data** - Setting the roles and policies is a big part of the equation, but you also need to prove that the controls are in place and were not violated. And in the case of breach, attack, or unintended disclosure, a detailed log report on who accessed what and when is necessary for investigative purposes. When implementing a solution for PCI; look for dashboards that can be customized to show access to credit card
Establishing a Process to Mitigate PCI Risk

During the course of preparation for the assessment or during normal operations, PCI risks may be uncovered. Also, as new threats and technologies emerge, new vulnerabilities may be exposed. For this reason it’s necessary to establish a process for mitigating the risk, and it helps to satisfy Requirement 12.5.3 “Establish, document, and distribute security incident response and escalation procedures.”

- **Involve End Users** - Risks that are related to broken business processes need to be investigated with the parties responsible for those processes before they are remediated to ensure that the remediation procedures will not interrupt the business. Providing details of why the process violates PCI can help the end user understand the issue so the IT team can work with them on a resolution.

A tool can help expedite this process by providing details on the owner of the document or application in question so they can be contacted and alerted to the PCI violation. Without the owner-related metadata that a tool provides it could take many hours of employee time to track down the owner and the longer it takes to find the owner, the longer it will take to remediate the problem and get the organization back in compliance.

Data monitoring and tracking tools can also provide a detailed flow analysis of who is using that data and when. Organizations can see if the data is part of an active business process or sitting in a rarely used data repository. Armed with detailed usage data, an owner can make more informed decisions about how to handle risks and manage the data in a PCI compliant manner.

- **Automate Workflow** - Managing the remediation process effectively requires tracking of actions and responses to ensure the risk is remediated and to provide accountability. Implementing automated solutions, where possible, improves efficiency and saves resource time.

Processes that can be automated include creation of a trouble ticket, reminders to the owner if the ticket is still open, and recording of the remediation changes made.

- **Track and Report** - Remediation actions and changes to systems in the CDE must be recorded to prove that the risk has been addressed. In addition to basic tracking and reporting, companies should build into the process full accountability tracking. There should be a full record of who authorized the change so they can be contacted if a change did not solve the problem or introduced another one.
Not every problem can be solved quickly. Some PCI issues involve payment applications that cannot be updated for months or multiple systems that require change approvals from a number of people. Use tracking and reporting to maintain a full record of the attempts at remediation and any compensating controls that were put in place to address the risk in the interim. Automatic tracking limits the chance that changes or updates that need to be delayed will be forgotten entirely. And full change reports can be presented to the assessor to prove remediation steps were taken.

Enforcing Controls to Prevent Leakage of Credit Card Data

The final piece of the puzzle is making sure all of the documented policy and procedure work is backed up by technical controls that enforce the policies in the CDE. Controls that are context aware will be able to protect data without interfering with business processes. For example, a solution that can accurately identify what is credit card data and what is just a 16-digit string of numbers can block outbound traffic that violates PCI while allowing traffic that doesn’t.

- **Existing Controls** - Most companies already have some form of role-based identity management (IdM) system in place. The IdM can be extended to the CDE to enforce things like “need to know” access, to restrict privileged IDs to least privileged use per Requirement 7.1.1 and to control creation, deletion, and changes to IDs per Requirement 8.5.1. If an organization has a network-based data leak prevention (DLP) tool, it can be used to monitor the perimeter of the CDE for credit card data. If the solution sees unencrypted cardholder data going across the perimeter as, for example, an email attachment, the email can be blocked or sent without the attachment. And a host-based DLP tool could be used on servers in the CDE to perform the same protective function.

- **Risk Based Enforcement Containment** - Some companies are unable to comply with all aspects of the PCI DSS testing procedures and need to implement compensating controls until they can change or mitigate the exposure. In these special cases, tools may detect and alert even though the exception has already been assessed and addressed using a compensating control. For example, the PCI DSS calls out the use of internal network segmentation, IP address filtering and two-factor authentication on the internal network as a compensating control for storage of unencrypted cardholder data. If the risk assessment has been made to accept this control, the monitoring and scanning tool alerts should be tuned accordingly.

Special Considerations

When using a tool to scan and possibly store credit card data keep in mind that the solution itself must be PCI compliant. A scanning tool that stores “matched” data that is credit card data needs to store it in a protected manner per Requirement 3. If the solution can’t do that, it could put the company using it out of compliance.

Other considerations include:

- **Role-based access control** - In order to support the “need to know” requirement, users of a scanning and discovery tool must either have legitimate business need to see the credit card data or the tool must be able to mask or otherwise prevent the person running the scan from viewing them. Or have different levels of privilege so multiple users could run the scan and see limited results but only certain privileged users can see the actual card data.

- **Multi-Factor Authentication** - If the scans will be run remotely, the tool must support two-factor authentication per Requirement 8.3.

- **Complete Visibility** - A thorough assessment requires full visibility into all of the systems in the CDE. This includes a method for monitoring all of the log data on servers and applications, all access to
sensitive information like cardholder data, change management for policies and settings and any configuration file changes.

- **Data Protection in Transit** - To protect any credit card data that goes to the scanning tool, findings must be transmitted using encrypted communication channels like SSL or IPSec.

- **Data Protection at Rest** - Any credit card numbers that are stored in the scanner need to be rendered unusable. This means they need to be stored encrypted. Alternately, they could be truncated or tokenized, but this may render the results of the scan less useful.

- **Key Management** - PCI requires that key management procedures must be implemented for protection of encrypted cardholder data. If the scanning tool stores the data encrypted, key management for the encryption keys must support all of the sub-requirements for Requirement 3.6 including: Generation of strong cryptographic keys, secure cryptographic key storage, cryptographic key changes for keys that have reached the end of their cryptoperiod and retirement or replacement of keys.

- **No Unnecessary Processes** - And since the system running the scan will have access to credit card data it needs to comply with Requirement 2.2.1 “only one primary function per server to prevent functions that require different security levels from co-existing on the same server.”

**The Five Steps At-a-Glance**

---

**Scope**
- Accuracy
- Scalability
- Coverage Breadth
- Minimum Impact

**Monitor**
- Accuracy
- Flexibility
- Non-Intrusive
- Alerting

**Repeatable Process**
- Tracking Progress
- Centralize Mgmt
- Historical Data
- Alerting

**Risk Mitigation Process**
- Involve End Users
- Automate Workflow
- Track and Report

**Control Enforcement**
- Existing Controls
- Risk Based Enforcement

**Special Considerations**
- RBAC
- Multi-Factor AuthN
- Complete Visibility
- Data Protection in Transit
- Data Protection at Rest
- Key Mgmt
- Nothing Unnecessary
Conclusion

Start by scoping. PCI causes a lot of compliance headaches but the process doesn’t have to be completely painful. With a little upfront planning and careful scoping, organizations can prepare themselves for the assessment and pre-check their own systems against the testing procedures as defined in v2.0 of the PCI DSS. Implementing the 5-steps of information and people centric approaches outlined in this report will help ease the compliance burden too.

There are many security tools that companies already have in place that can be used to protect credit card data when extended into the CDE. And a robust information governance and data protection program should position a company well for PCI compliance. In other words, if an organization has already completed the work for segmenting the network and protecting sensitive data, the building blocks for passing the PCI assessment are already in place and only minor adjustments or additions will be needed for the RoC validation.

The most important first step, after reading the PCI DSS is to find all the credit card data in your enterprise and make sure none of it is stored outside of the CDE. Inside the CDE, monitor access to the data and prevent or alert on any unauthorized attempts to move it out of the CDE. PCI compliance still won’t be easy for most, but controlling scope by control the credit card data itself will make it less time-consuming and reduce the chance of “gotcha” findings during the assessment.
About the Author

Diana Kelley is a Principal Analyst at SecurityCurve and has extensive experience delivering strategic, competitive knowledge to large corporations and security software vendors. She was Vice President and Service Director for the Security and Risk Management Strategies (SRMS) service at Burton Group, the Executive Security Advisor for CA’s eTrust Business Unit, and a Manager in KPMG’s Financial Services Consulting organization.

diana@securitycurve.com
@securitycurve
www.securitycurve.com

References & Resources


