

PCI Compliance: Best Practices for Securing Credit Card Data

by Jeremy Simon, PCI QSA, CISSP, CISA

Mandated since June, 2001, the Payment Card Industry Data Security Standard (PCI DSS) specifies a broad range of technical, administrative and physical security controls for protecting credit card data. While the PCI DSS is made up of only 12 main requirements, they are divided into over 200 sub-requirements, all of which must be satisfied in order to be considered fully compliant.



The PCI DSS provides a well-defined list of security requirements, but many organizations are left with more questions than answers when it comes to determining how best to address each requirement in a manner that will be considered acceptable for PCI compliance.

When approaching PCI compliance, much of the effort can often be handled in-house, but it's also important to know when to ask for help. Misinterpretation of PCI requirements may lead to costly mistakes. To address the need for expert guidance, the PCI Security Standards Council maintains a program for training Qualified Security Assessors (QSA's). A QSA is not intended to be merely an auditor, but is also meant to act as an advisor to organizations working to achieve PCI compliance. QSA's are trained to provide clarification of the underlying intent of the PCI requirements and to assist organizations in identifying reasonable means of satisfying PCI obligations.

The following step-by-step approach for becoming PCI compliant will help the organization avoid many of the pitfalls commonly associated with the process:

- 1. Educate Yourself**

Read the PCI DSS, preferably several times. Ensure you understand each requirement and try to see the underlying intent of each. Make a list of all the questions you have. Read PCI related forums and blogs to see how other companies are addressing PCI compliance issues. It's often helpful to engage a QSA (PCI Qualified Security Assessor) at this point, to provide direction and answers to questions that will inevitably arise during the process of becoming PCI compliant.

- 2. Determine Your PCI Classification**

Work with your acquiring bank to determine what Merchant or Service Provider classification level applies to your organization for compliance validation purposes. Each acquiring bank is responsible for ensuring the compliance of all of its merchants, so the bank has the authority to determine your company's PCI classification level. A QSA can help you determine what classification will likely be assigned based upon acceptance channels and transaction volume, but in the end, the bank has the final say in this regard.

- 3. Perform Data Discovery**

Find out where cardholder data currently exists in your environment. Identify all payment acceptance channels, map out the flow of cardholder data across the network, and identify all places where that data is stored. It is helpful to create a network topology diagram that shows

network segments where key systems reside – then map the cardholder data flow onto this diagram for a visual representation of where credit card data is transmitted, processed or stored in your network.

4. **Whenever Possible, Eliminate Cardholder Data Instead of Securing It**

Securely dispose of any cardholder data that is not required. This may help to reduce the scope for PCI compliance and will likely reduce the costs associated with becoming compliant. Most companies will still need to retain credit card data, but should make sure it's stored in a centralized, tightly controlled manner. Some organizations that handle only a small volume of transactions may find that it's easier and less expensive to completely outsource all credit card processing to a third party. If this approach is used, PCI compliance requirements may no longer apply at all (check with your banking institution to be sure).

5. **Define the Scope for PCI Compliance**

Now that you know where the cardholder data exists, who has access to it, and how the network is segmented, the scope for PCI compliance can be determined. The entire enterprise (both in terms of network and staff) may not necessarily need to be included within the scope of PCI compliance – and proper scoping is essential to controlling costs for PCI compliance! The PCI DSS applies to all systems that store, process or transmit cardholder data, as well as any systems connected to those (in other words, other systems on the same network segment, not separated by a firewall). Since scope is such a critical aspect of PCI compliance, this is a good point to confirm your scoping approach with a QSA to ensure it will be considered acceptable by PCI standards.

6. **Perform a Gap Assessment**

Perform a gap assessment based upon the established PCI scope. Determine whether each requirement is satisfied for all in-scope systems. The PCI Audit Procedures provide additional details regarding how to validate the presence of each required control. Every single requirement must be addressed for full compliance – but compensating controls are allowed, as long as certain criteria are met (see PCI DSS, Appendix B).

7. **Implement Changes to Address Non-Compliant Findings**

Build a remediation plan to address non-compliant findings. Implement required controls, write policies, update legal contracts, etc. This step can often turn into an extensive process, depending on the present state of information security and governance in your organization. PCI requirements include technical, physical and administrative controls, so organizations without a well developed InfoSec program will find there's a lot to be built in order to address PCI requirements. This is another point where it makes sense to work with a QSA. A good QSA should be able to help you come up with a cost effective remediation strategy that is appropriate for your particular business.

8. **Perform Quarterly Vulnerability Scanning and Annual Penetration Testing**

Find an Authorized Scan Vendor (see URL below) to scan all Internet accessible systems on a quarterly basis. Remediate any non-compliant findings and rescan until a fully compliant scan report is obtained. In addition to quarterly vulnerability scanning, organizations must also perform penetration testing (network & application layers) at least annually or when significant changes are made to the environment.

9. Provide Validation of PCI Compliance

Have an on-site audit performed, or complete the self-assessment questionnaire. Submit the Report on Compliance or Self-Assessment Questionnaire, along with the quarterly scan results, to your acquiring bank (for merchants) or to Visa (for service providers).

10. Stay Compliant through Ongoing Security Maintenance

Maintain security controls according to guidelines outlined in the PCI DSS to ensure ongoing compliance. There is “safe harbor” protection for organizations who can demonstrate that they were in full compliance with the PCI DSS *at the time of a breach*. This is why it’s important to not only *become* compliant, but also to *stay* compliant.

The following are additional reference materials that are available online and may be useful:

- www.pcisecuritystandards.org – This is the official PCI Council website, where you can find all of the official documents related to PCI. You’ll want to download and read at least the following:
 - PCI DSS v1.1
https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf
 - Audit Procedures
https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf
 - Self-Assessment Questionnaire
https://www.pcisecuritystandards.org/pdfs/pci_saq_v1-0.pdf
- Visa CISP program overview
http://usa.visa.com/download/merchants/cisp_overview.pdf
- <http://pcianswers.com/> -- A great PCI-related blog, managed by reputable QSA’s
- pci.halock.com – Halock’s PCI Compliance Portal – knowledge-base, news articles, and task management for PCI related activities
- List of Qualified Security Assessors
https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- List of Authorized Scanning Vendors
https://www.pcisecuritystandards.org/pdfs/asv_report.html

About the Author:

For the last ten years, Jeremy Simon has served as Partner and CTO of Halock Security Labs. With over 15 years of experience in information security consulting, Jeremy’s primary focus in recent years has been providing PCI compliance advisory services, and he has worked with companies of all types and sizes in achieving PCI compliance.

About Halock Security Labs:

Halock Security Labs is a professional services organization focused 100% on information security. Halock’s core services include Assessments, Governance & Strategy, Network & Systems Security, as well as Application Security. We are in partnership with our clients to help them protect critical information assets and to satisfy compliance requirements and/or international security standards.

<http://www.halock.com>

