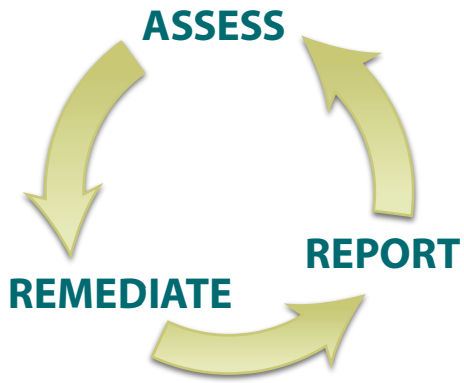
Getting Started with PCI Data Security Standard

Data security for merchants and payment card processors is the vital byproduct of applying the information security best practices found in the Payment Card Industry Data Security Standard (PCI DSS). The standard includes 12 requirements for any business that stores, processes or transmits payment cardholder data. These requirements specify the framework for a secure payments environment, but for purposes of PCI DSS compliance, their essence is three steps: Assess, Remediate and Report.

PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS



Assess is the process of taking an inventory of your IT assets and business processes for payment card processing, and analyzing them for vulnerabilities that could expose cardholder data. **Remediate** is the process of fixing those vulnerabilities. **Report** entails the compilation of records required by PCI DSS to validate remediation, and submission of compliance reports to the acquiring bank and card payment brands you do business with. Doing these three steps is an ongoing process for *continuous* compliance with the PCI DSS requirements. These steps also enable vigilant assurance of cardholder data safety.

"PCI DSS represents the best available framework to guide better protection of cardholder data. It also presents an opportunity to leverage cardholder data security achieved through PCI DSS compliance for better protection of other sensitive business data – and to address compliance with other standards and regulations."

AberdeenGroup
IT Industry Analyst

PCI Data Security Standard Requirements

PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards, and to store, process, and/or transmit cardholder data. It presents common sense steps that mirror best security practices.

Goals	PCI DSS Requirements – Validated by Self or Outside Assessment
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 passwords and other security parameters
Protect Cardholder Data	3. Protect stored 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 all personnel

Step 1 – Assess

The primary goal of assessment is to identify all technology and process vulnerabilities posing a risk to the security of cardholder data that is transmitted, processed or stored by your business. Study the PCI DSS on our web site (www.pcisecuritystandards.org) for detailed requirements. It describes IT infrastructure and processes that access the payment card infrastructure. Determine how cardholder data flows from beginning to end of the transaction process – including PCs and laptops which access critical systems, storage mechanisms for paper receipts, etc. Check the versions of personal identification number (PIN) entry terminals and software applications used for payment card transactions and processing to ensure they have passed PCI compliance validation.

HOW TO ASSESS PCI DSS SECURITY

Study PCI DSS Standard

Learn what the standard requires of your business

Inventory IT Assets and Processes

Identify all systems, personnel and processes involved in the transmission, processing or storing of cardholder data

Find Vulnerabilities

Use the appropriate SAQ to guide the assessment, and appropriate technologies to locate insecure systems

Validate with Third-Party Experts

Your environment's complexity may require a Qualified Security Assessor and/or Approved Scanning Vendor to execute proper assessment

PCI SSC FOUNDERS

PARTICIPATING ORGANIZATIONS

Merchants, banks, processors, developers and point of sale vendors

Note: your liability for PCI DSS compliance also extends to third parties involved with your process flow, so you must also confirm that they are compliant. Comprehensive assessment is a vital part of understanding what elements may be vulnerable to security exploits and where to direct remediation.

Self-Assessment Questionnaire (SAQ). The SAQ is a validation tool for eligible merchants and service providers who self-evaluate their PCI DSS compliance and who are not required to submit a Report on Compliance (ROC). A number of SAQs are available for different environments; see table below and our web site for details:

SAQ	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. *This would never apply to face-to-face merchants.*
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	All other merchants not included in descriptions for SAQ types A through C above, and **all service providers** defined by a payment card brand as eligible to complete an SAQ

Qualified Assessors. The Council provides programs for two kinds of independent experts to help with your PCI assessment: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs have trained personnel and processes to assess and prove compliance with PCI DSS. ASVs provide commercial software tools and analysis services for performing external vulnerability scans for your systems. The PCI SSC also provides educational resources for merchants and service providers, including training for Internal Security Assessors (ISAs). Visit our Web site at www.pcisecuritystandards.org for details and links to qualified assessors and training resources.

Step 2 – Remediate

Remediation is the process of fixing vulnerabilities – including technical flaws in software code or unsafe practices in how an organization processes or stores cardholder data. Steps include:

- Scanning your network with software tools that analyze infrastructure and spot known vulnerabilities
- Review and remediation of vulnerabilities found in on-site assessment (if applicable) or through the self-assessment process
- Classifying and ranking the vulnerabilities to help prioritize the order of remediation
- Applying patches, fixes, workarounds, and changes to unsafe processes and workflow
- Re-scanning to verify that remediation actually occurred

Step 3 – Report

Regular reports are required for PCI DSS compliance; these are submitted to the acquiring bank and payment card brands that you do business with. PCI SSC is not responsible for enforcing PCI DSS compliance. All merchants, service providers and processors may be required to submit quarterly scan reports, which must be performed by a PCI SSC approved ASV. Businesses with larger transaction volumes have an annual on-site assessment completed by a PCI SSC approved QSA and submit the findings to each acquirer. Businesses with smaller transaction volumes may be required to submit an annual Attestation within the Self-Assessment Questionnaire. For more details on validation and reporting requirements, speak with your acquirer or payment card brand. Please also visit our web site at: www.pcisecuritystandards.org.