



PCI - Network Assessment and Compliance

360 GRC
Whitepaper



Audit IT, Trend IT, Solve IT

What is the history behind PCI compliance?

PCI DSS originally began as five different programs: Visa Card Information Security Program, MasterCard Site Data Protection, American Express Data Security Operating Policy, Discover Information and Compliance, and the JCB Data Security Program. Each company's intentions were roughly similar: to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data.

The Payment Card Industry Security Standards Council (PCI SSC) was formed on December 15, 2004. These companies aligned their individual policies and released the Payment Card Industry Data Security Standard (PCI DSS). In September 2006, the PCI standard was updated to version 1.1 to provide clarification and minor revisions to version 1.0. Version 1.2 was released on October 1, 2008. Version 1.1 "sunsetting" on December 31, 2008. Version 1.2 did not change requirements, only enhanced clarity, improved flexibility, and addressed evolving risks/threats. In August 2009, the PCI SSC announced the move from version 1.2 to version 1.2.1 for the purpose of making minor corrections designed to create more clarity and consistency among the standards and supporting documents.

PCI DSS -- What is it?

The Payment Card Industry Data Security Standard (PCI DSS) is a multi-faceted security standard that includes comprehensive requirements for security management, policies, procedures, network architecture, software design and other critical protective measures for enhancing payment account data security assembled by the Payment Card Industry Security Standards Council (PCI SSC). Visa, American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International were to provide a 'minimum security standard' with regards to cardholders' account and transaction information and help facilitate the broad adoption of consistent data security measures on a global basis.

The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls and eliminate its exposure to compromise. The standard applies to all organizations that hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

Validation of compliance can be performed either internally or externally which depends on the volume of card transactions the organization is handling. Regardless of the size of the organization, compliance must be assessed on an annual basis. Organizations handling large volumes of transactions must have their compliance assessed by an independent assessor known as a Qualified Security Assessor (QSA), while companies handling smaller volumes have the option of self-certification via a Self-Assessment Questionnaire (SAQ). In some regions these SAQs still require signoff by a QSA for submission.

The bodies holding relationships with the in-scope organizations do enforcement of compliance. For organizations processing Visa or MasterCard transactions, the organization's acquirer enforces compliance, while the organizations handling American Express transactions will deal directly with American Express regarding compliance. In the case of third party suppliers such as hosting companies who have business relationships with in-scope organizations, enforcement of compliance falls to the in-scope company, as neither the acquirers nor the card brands will have appropriate contractual relationships

PCI Compliance

in place to mandate compliance. Non-compliant companies who maintain a relationship with one or more of the card brands, either directly or through an acquirer risk losing their ability to process credit card payments and being audited and/or fined.

PCI: What does it mean to you?

If your business is involved in accepting credit or debit card payment thereby transmitting, processing, collecting or storing credit card transaction information, then **YOU MUST COMPLY WITH PCI**. The cost of assessing your network to comply with PCI DSS pales in comparison to the cost of compromising the credit card numbers of your customers. Below are a couple of instances of credit card theft:

- In the world's most well known theft of credit-card information, cyber thieves launched an internet-based attack on a major national discount clothing retailer. A planned attack began in July 2005 and continued throughout 2006. By the time the cyber-attack was discovered, the thieves had managed to steal at least 46 million credit and debit card numbers, along with military identification and Social Security numbers of several hundred thousand customers. This attack served as a public case for PCI compliance. Journalists from mainstream newspapers all over the world reported that the thieves had taken advantage of the retailer's poorly protected network. The financial costs of the massive attack are still not clear, but it's safe to say the retailer is still looking at hundreds of millions of dollars in breach-related expenses — including several class-action lawsuits.

- In 2005, with similar methods, cyber thieves gained access to the customer databases of a national shoe retailer, and stole 1.4 million credit card numbers along with the names on those accounts. The theft affected 108 stores in 25 states.

What is at stake if you don't follow the rules?

Compliance under PCI DSS is **mandatory**, with violations carrying severe penalties. While the PCI data security standard provides a common set of security requirements for all the major electronic payment brands, each individual credit card company is entrusted to enforce the compliance with its respective customers. Each major credit card company is very serious about enforcement.

The reimbursement of consumers will have a major financial impact on the companies. In fact, compliance audits are becoming more and more commonplace, as the industry works to prevent massive security breaches from happening in the future. A retailer that is found to be non-PCI-compliant will face stiff penalties from the credit card company, regardless of whether the network has been compromised. Such penalties can include:

Hefty Fines - Both VISA and MasterCard have published fine schedules for PCI. Under VISA operating regulations, members may be assessed fines for data compromise or non-compliance with PCI requirements. The first violation will receive fines up to \$50,000 for a rolling 12 month period or until the merchant demonstrates that all non-compliance have been remediated. A second violation will incur \$100,000 for a 12 month rolling period. Third violation details are at management's discretion. The MasterCard fine structure is slightly different, but merchants should expect initial fines of up to \$100,000 and \$10,000 per day after 60 days, not to exceed \$500,000 annually.

PCI Compliance

Sole Liability - Historically, credit card companies have borne the brunt of the liability of electronic data theft. But today, if a retailer is the victim of a credit card security breach, the credit card provider is generally liable only if the retailer was PCI compliant at the time the security breach occurred. Otherwise, the retailer will face a very expensive case of “we told you so.” In addition to fines, non-compliant retailers face numerous damage control fees for compensating customers whose cards have been compromised. For example, most credit card companies charge a fee to reissue a new credit card or card number. That fee per customer is often nominal — around \$25 per customer. But if a retailer is paying said fee for a million compromised customers, then that fee isn’t a nominal penalty anymore.

The right to revoke a retailer’s ability to accept credit cards - If a retailer flouts PCI compliance, a credit card company may expel a retailer from its program, prohibiting that retailer from accepting its credit cards anymore. This will have a significant impact on a company’s revenue generation.

Loss of client confidence - The loss of business due to an unforeseen confidential data loss or a security breach can be permanent. The publicity alone can have a devastating effect. Data that is destroyed is seen within any industry as poor business process and loss of consumer confidence is evident.

Data Breach Notification Laws - Now consider that while you may have the same devastating business loss as you suffered above, with a data breach, your company may now have additional and expensive responsibilities. If the data that was lost is considered confidential and consumer related, it is considered a Security Data Breach that may require a company to conform to any number of Data Breach Notification Laws or risk federal or state penalties. The notification process is very expensive; current estimates are over \$200.00 per account lost, and penalties and fines are starting to increase to unrecoverable amounts.

Increased/Decreased Fees - Compliance has its privileges, and some credit card companies are making a point not only to penalize retailers who don’t comply with the PCI standard, but to reward those who do comply. For instance, some credit card companies have said that they are considering raising the percentage-based fee per transaction that all retailers pay every time a customer uses a credit card, but that they will keep the percentage rate low for those customers who can prove PCI compliance.

So what are you required to do to comply with PCI mandates?

The PCI DSS framework is divided into 12 security requirements (VISA refers to them as the ‘Digital Dozen’) that are organized in six categories as follows:

1. *Build and maintain a secure network*

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

2. *Protect cardholder data*

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

3. *Maintain a vulnerability management program*

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

4. *Implement strong access control measures*

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

PCI Compliance

Requirement 9: Restrict physical access to cardholder data

5. ***Regularly monitor and test networks***

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

6. ***Maintain an information security policy***

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

Can an audit be performed on the network to ensure PCI DSS compliance?

Unfortunately, most PCI covered entities are not placing any emphasis in complying with PCI on the network. A minority of covered entities are trying to comply by manually auditing their network configurations or using a home grown script to inspect individual device settings. To ensure 100% compliance, the Information Risk Professional should review each line of every network device's configuration file and try to ensure that it matches the applicable PCI mandates.

There are several potential risks and problems with this approach:

- The process can be tedious and time consuming, even in small IT environments. Therefore audits are not performed or only in a minimum number of network devices. This can expose non-compliance with the remaining devices.
- The process leaves much room for error, as it's easy to overlook a device or setting due to the technical nature of the review.
- Performing routine audits can be costly and difficult, especially in large environments in which changes are frequent and thousands of devices must be examined.

Summary

Although some vital differences exist among the various regulations, all share one unifying factor: they all deal with fundamental issues of data security and privacy. In IT, an optimal way to address regulations is first to understand the potential threats and vulnerabilities of the data and the network then create an effective and secure technology solution built on a well-designed infrastructure.

This approach enables an organization to easily deal with any new regulations that become law. Many organizations have invested in well-designed network infrastructures, but they still need an upgrade or a technology refresh to achieve a comprehensive solution to meet their regulatory compliance challenges.

About 360 GRC

360 GRC is headquartered in Manhattan, New York. 360 GRC's management team includes over 100+ years in global enterprise Architecture and over 50+ years in IT Audit and IT Security field in top global organizations.

To learn more, visit www.360grc.com
© 2010, 360 GRC Inc.

The information contained herein is subject to change without notice. The only warranties for 360 GRC products and services are forth in the express warranty statement accompanying such products and services. 360 GRC shall not be liable for technical or editorial errors or omissions contained herein.