

Guide to passing PCI's five toughest requirements

It is well known by now that the major credit card companies have collectively mandated that all members, merchants and service providers storing, processing or transmitting cardholder data must adhere to the Payment Card Industry (PCI)'s "12 commandments" -- the dozen overarching best practices that make up the guideline -- or else risk possible fines and even the termination of credit card processing privileges. Unfortunately, the path to PCI DSS compliance can be demanding due to the amount of money, time and effort required.

This learning guide will review a few of the more challenging PCI DSS requirements and provide some tips that enterprises can use to achieve PCI DSS compliance.

PCI DSS: Where are organizations struggling?

All of the PCI DSS requirements seem to be fairly well defined, unlike those of the Sarbanes-Oxley Act. SOX does not provide any specific direction on how to secure information assets and has been open to varying interpretations by companies and compliance audit firms. Nevertheless, organizations still find it difficult to become PCI DSS compliant. In an interesting study conducted by VeriSign Inc., researchers found that organizations were most likely to be noncompliant with PCI Requirement 3. Seventy-nine percent of the failed assessments did not meet the requirement to protect stored data. According to VeriSign, the top five PCI assessment failings were:

Requirement 3: Protect stored data	79%
Requirement 11: Regularly test security systems and processes	74%
Requirement 8: Assign a unique ID to each person with computer access	71%
Requirement 10: Track/monitor network resources and cardholder data	71%
Requirement 1: Install and maintain a firewall configuration to protect data	66%

The Slaughterhouse-Five: Why are these problem areas?

Regardless of the fact that PCI DSS is definitely comprehensive, the list of requirements allows for 12 potential points of failure; the inability to pass any one means an organization won't be compliant. Additionally, even with the PCI DSS providing specific requirements, it can be interpreted differently by different types of organizations. Let's review the aforementioned PCI requirement failures, analyze why these might cause trouble for some organizations and discuss what measures can be taken to resolve the dilemma.

A GUIDE TO PASSING PCI'S FIVE TOUGHEST REQUIREMENTS

- [Requirement 3: Protecting stored data](#)
- [Requirement 11: Regularly test security systems and processes](#)
- [Requirement 8: Assign a unique ID to users](#)
- [Requirement 10: Monitor access to network resources and data](#)
- [Requirement 1: Install and maintain a firewall configuration](#)
- [Conclusion](#)

PCI DSS Requirement 3: Protecting stored data

From the very instant that a merchant receives a customer's credit card information, all of the card data must be encrypted. In a National Federation of Independent Business/Visa survey that was presented at Visa's March 2007 conference, small business owners said that they believe they are doing a good job of securing customer data, despite frequent evidence to the contrary. Among the respondents that said they retained their customers' data, more than 25% kept customer records in unsecured files, and 36% of those surveyed accepted credit card numbers at their stores.

One of the biggest problems with this requirement is that merchants must accurately know where credit card data flows from its inception, where it traverses the network and resides, and what its "state" is along the way. This is why it is critical to identify and examine all desktops, laptops, servers and databases that handle any type of cardholder information. This includes all of the database files and/or SQL tables that contain credit card numbers, not to mention all of the application systems that create or access credit card numbers. No matter what type of system touches the credit card information, it must be protected by encryption.

How to pass PCI requirement 3:

As mentioned above, start identifying all of the systems that touch cardholder data because these systems will be included in the scope of an eventual PCI DSS audit or compliance validation. It is also important to understand the compartmentalization of the cardholder systems and how they are using firewalls and network filter controls. Such an arrangement may dictate if nearby systems would also be within the scope of a PCI DSS compliance validation. You may be surprised to find out that the total number of systems retaining cardholder data -- including data warehouses, development servers, middleware and backup systems -- is quite large.

Next, document the flow of credit card data throughout your organization and identify the business functions. The marketing department, for example, may need customer data, but not the associated credit card information. Track data from the point of acquisition -- even from customers or 3rd parties -- to the point where the data is disposed of or leaves the corporate network. Also be sure to identify all of the computers and networks that connect to the organization's infrastructure and applications. These can include network connections from business units, vendors, partners and the systems of remote employees. All fluid credit card data should be encrypted using methods such as SSH, VPN, or SSL/TLS for encryption.

If you are not confident in your IT department's ability to accurately identify sensitive data, there are very good data loss prevention tools that can assist in this effort. These tools are designed to sift through data across the enterprise and accurately report on which systems house it, where it is on the system and who has access to it. Once known, review the organization's access controls to enforce "need to know" policies. Also, see if it is possible to minimize how many and which systems have this sensitive information.

PCI DSS Requirement 11: Regularly test security systems and processes

Many organizations perform little or no regular testing on the adequacy of the security controls governing their network and Internet-facing Web site applications. Failure to periodically run internal and external network scans to identify weaknesses can prove costly when back doors are left open to hackers and malicious code. Organizations may be protected at a given moment, but new vulnerabilities appear daily, which is why networks should be consistently patched and hardened. According to the [National Vulnerability Database](#) provided by the Department of Homeland Security's National Cyber Security Division, an average of 19 new vulnerabilities are posted to the Internet daily.

One good example of the need for the regular testing of systems and processes is the recent data security breach at TJX Companies Inc. The TJX breach was ultimately caused by an insecure wireless network. According to a Wall Street Journal report, investigators believe that the hacker was able to use a laptop and a telescope-shaped antenna to bypass older security technology and penetrate the WLAN network. The \$17.4-billion retailer's wireless network had less security than many people have on their home networks. For 18 months, TJX had no knowledge that it had been compromised, allowing malicious hackers to download at least 45.7 million credit and debit card numbers.

How to pass PCI requirement 11:

When it comes to scanning your information systems for vulnerabilities, make certain to use tools and techniques that expose vulnerabilities in devices on wired or wireless networks. There are an enormous number of security risks linked to wireless protocols, weak encryption methods and the lack of employee security awareness. Cracking methods have become much more advanced and can be carried out with open source tools freely available on the Web.

A substantial number of successful attacks are carried out against systems that do not get patched with the latest security updates. In addition to a systematic patching process, the greatest protection against network and application security threats is the consistent use of vulnerability scanners that can see all of the applications and devices on a network, identify vulnerabilities and supply remediation information. Nevertheless, scanning the corporate network for vulnerabilities will not reveal everything and may only uncover issues that have already been confronted or at least discovered. Scanning, though helpful, may not necessarily offer what a real, attack-like penetration testing program provides.

In order to be aware of its readiness, it is imperative (and required by the PCI DSS) that an organization perform an annual penetration test on its information systems, measuring how well the systems can endure an attack. This type of test actually exploits vulnerabilities to better quantify the true risk of any particular finding. According to a report found in The Retail Data Security 2005 Benchmark Study, only 51% of retailers perform network penetration testing. A frightening 14% of the survey respondents indicated that they had suffered a customer data security breach. Vulnerability scanning provides a look into known weaknesses, but does not address the elements of a successful intrusion. Your testing should include a deeper dive that will bring to light the real threats to your organization's assets.

Furthermore, when it comes to testing processes, all changes that could affect ingress and egress filter rules should go through a formal process before adjustments are made to firewalls, routers, VPNs and WLAN devices. These changes should be reviewed carefully for proper justification, and management must be made aware of any newly discovered security risks. Information systems environments will always have to change in order to help the business obtain its objectives; therefore, all changes must continually be reviewed and fully documented.

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

A critical concern of PCI compliance is traceability and accountability of who did what and when. Even though organizations realize that the main techniques used to address this requirement are user and password management, both of these techniques are difficult to implement. To do so, incorporate tools that automate these tasks, or assign technical staff to handle them. Large networks can have heterogeneous environments with many points of entry, including firewalls and VPN access. The various options make it difficult to track user accounts and behavior on information systems without the proper infrastructure. These same organizations may not be monitoring domain password policies correctly for all changes.

How to pass PCI Requirement 8

Organizations must be able to identify and log all user and administrative access to information systems and applications containing credit card information. Organizations must create a unique ID for every individual that will have computer access. The company must also possess a documented policy -- signed by all employees -- pointing out that all IDs and credentials are to be used only by the people to whom they are specified. Organizations need to be capable of verifying who is attempting access to an asset. They also must control what employees are permitted to see or modify, and do so based on their organization role.

Management must make sure that it enforces a policy for aging passwords. As an example, if a company has a policy that states all passwords will be changed every 45 days, they must be able to demonstrate that this actually occurs. Additionally, organizations have to be able to show that there is a repeatable process in place for providing passwords for new employee hires, as well as removing passwords when an employee no longer works for the organization.

PCI DSS also requires two-factor authentication to identify remote users that need to access resources, whether they are employees, administrators or third parties. While account name and password is typically the easiest and least expensive method of network logon authentication, organizations have now started to realize the weaknesses of this method. Passwords can be guessed or cracked using dictionary attacks, or users can be tricked into disclosing their passwords to other people. One way to stop social engineers and reduce additional risks associated with passwords is to apply two-factor authentication. If users are obligated to type in a password and provide additional information, such as a PIN from a card or token, then a hacker would not be able to get into the network with a password alone. Two-factor authentication can be established by using the combination of something a user knows (a password, for example), something a user possesses (ATM card), or something the user is (fingerprint).

Finally, it is crucial that organizations use an enterprise-wide authentication framework that will control how users can securely connect to the network. The framework, which can be built or bought, should not only be used to authenticate users to resources, but can also help limit access to resources based on business requirements. Doing so requires the development of a set of repeatable processes, along with technologies and policies that will protect user identities and data. Limiting users to a "need to know" basis helps to eliminate risk.

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

Many organizations have disparate networks and must manually track each system's log files in order to comply with PCI DSS. Individually sifting through system logs can not only be an extremely time-consuming process, but the task can also be a major drain on IT, especially when you need to determine the cause of a compromise. Organizations have to track and monitor all access to network resources and cardholder data, including real-time, daily and active events. Aside from managing these logs, most organizations don't have a good policy that addresses the various types of information being logged, and companies have no way of sustaining the integrity of the logged data. When it comes to having access to credit card data, organizations should not only have audit trails in place, but they should also only provide this kind of sensitive information to people who absolutely need to know it.

How to pass PCI Requirement 10

Even though analyzing logs and event data analysis is directly specified in the PCI DSS, it is simply good practice for any organization to monitor events. In an average information systems environment, event data is distributed, very large and at times hard to decipher. Most operating systems, by default, have utilities that analyze events, but they only offer basic features. Consequently, there is often no way for IT personnel to be alerted when specific critical events are logged, such as the unauthorized access of cardholder information. For the most part, the event browsing and filtering capabilities provided by these tools are restricted.

However, there are a number of impressive software- and hardware- based security information management (SIM) products that provide comprehensive log management. SIM tools can centralize events, automate the aggregation and correlation of event data, issue alerts and provide extremely detailed reporting capabilities. While aggregating events, SIMs will not only assist in creating a baseline of normal network activity, but they will also provide built-in rules to categorize them, triggering alerts and procedures as a result. Many security information management products also provide default rule sets that classify events according to PCI requirements.

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

At first glance, security professionals look at this requirement, simply install a firewall on their network perimeter and then think that all is well. Not quite. Many people fail to realize that PCI DSS Requirement 1 states that organizations must not only have a working firewall that is configured and documented correctly for ingress and egress filtering rules, but also utilize trusted zones (such as DMZs) and the use of perimeter firewalls installed between wireless networks and the cardholder data environment. These are just a few of the many specific details within the first PCI DSS requirement that tend to get ignored

How to pass PCI Requirement 1

Organizations need to thoroughly review firewall configurations and the policies that control the traffic flowing into and out of a network. Many firewalls go untouched for quite some time after their initial network installation. Because business application needs and customer requirements change over time, many rules are adjusted to allow for additional ports and services to be initiated, allowing open communication between trusted and untrusted segments.

All changes on these devices must be approved, accurately documented and reviewed on an ongoing basis to make sure that they are hardened and only allow secure information to flow between network segments. Documented configuration standards for these protections are mandatory along with specific documentation that justifies your network practices.

Finally, do not forget that configurations must provide security for assets that store, transmit or process cardholder data, which includes the appropriate network segmentation of information from wireless and mobile devices.

Conclusion: The Risk Mitigation Challenges of the "12 PCI Commandments"

PCI is designed to safeguard credit card data from the time it is received until the end of its life cycle. The stakes are high for organizations like Internet-based businesses, which rely heavily on credit card processing to sell products and services. It only takes one security breach to cause significant harm to a business's bottom line as well as its reputation, and that harm can be permanent.

Understanding which requirements of the "12 commandments" are the most challenging can help your organization to avoid wasting time, money and effort on the wrong ideas or technical implementations.

Furthermore, it is important to know that the PCI isn't concerned with how many employees you may have or what your annual revenue is; therefore, organizations must look at the requirements not simply as a checklist, but as a practical guide to developing a risk management program. Implementing sound security policies, utilizing technologies for log and vulnerability management, properly building network segmentation and securing the perimeter through the use of firewalls can go a long way toward helping an enterprise achieve PCI compliance.

ABOUT TBG SECURITY

TBG Security provides compliance services the Fortune 1000, as well as other leading retail, education, healthcare and telecommunications companies. TBG Security is engaged by leading companies around the world, including: Partners Healthcare, Bahamas Telecommunications Company, US Fiduciary Service and more. TBG Security Compliance Services provides a complete spectrum of compliance management consulting and integration services, including payment service integration, risk management compliance administration, automation and payment security compliance.