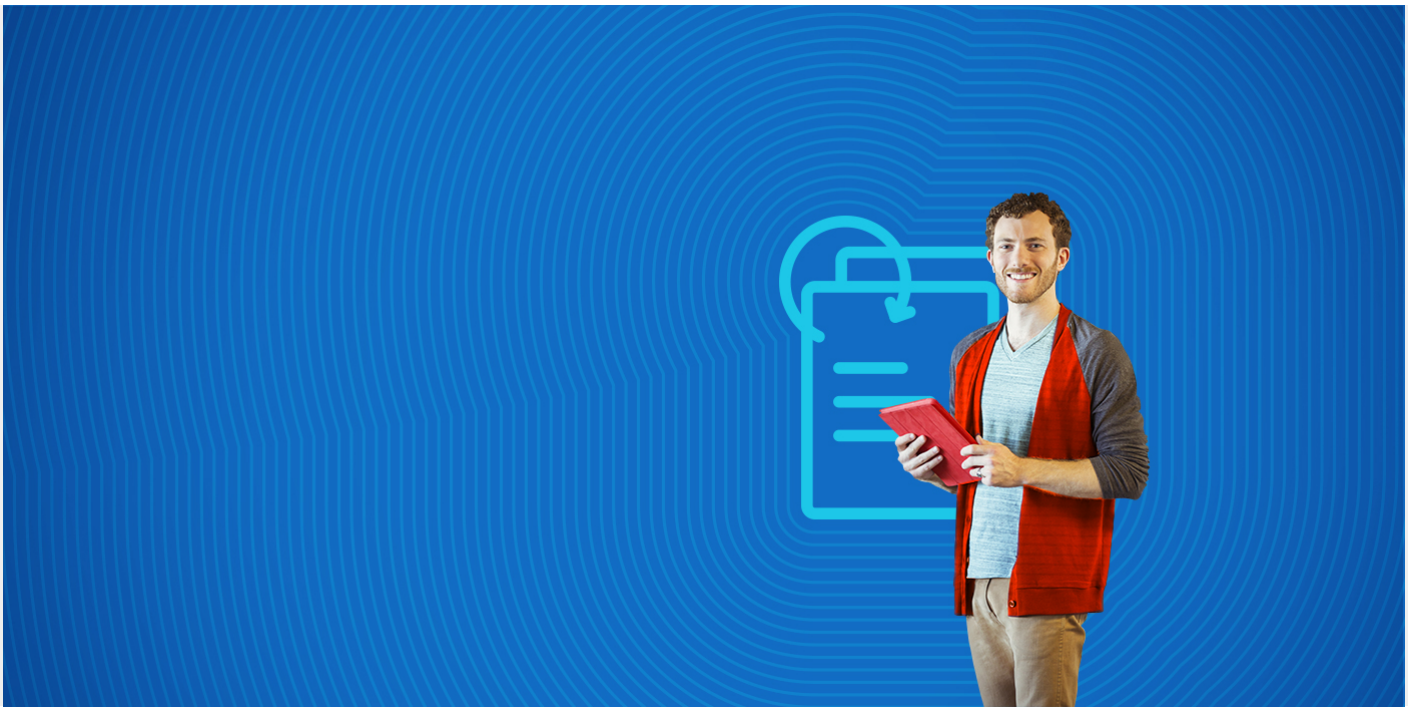
INTRODUCTION TO PCI COMPLIANCE



What is PCI DSS?

Payment Card Industry Data Security Standards, or PCI DSS, are a group of security regulations created to protect consumer privacy when personal credit card information is transmitted online and stored or processed by businesses. The PCI DSS helps circumvent security breaches and identity theft across e-commerce platforms. Businesses who deal with credit card information are required to be PCI compliant, but the rules can be confusing. This article explains what the PCI DSS is, why it is important and what businesses need to know in order to abide by the standards.

Every merchant , no matter how big or how small, is obligated to comply with 250 regulations set forth by the PCI DSS. It's important for companies to understand what the PCI DSS is and the significance of abiding by the rules.

With the development of e-commerce and the Internet, credit card brands have dealt with an increasing amount of fraud. Before the 21st century, the credit card companies were usually liable, and the expense of covering fraudulent charges was mounting quickly across the board. The chief credit card brands resolved to induce change at the merchant level to implement additional safeguards that would prevent fraud from occurring and spread out some of the liability concerns.

At first, the rules were applied by the credit card companies themselves. However, this led to inconsistencies and varying standards, and merchants were confused as to how they could abide by the rules.

In 2004, the card companies decided to work together to create a unified security standard, and the first version of the PCI DSS was born. Two years later, the five major credit card brands, Visa,

MasterCard, American Express, Discover and JCB International, created and sponsored the PCI Security Standards Council, an autonomous group responsible for continuing to develop and manage the standards and educate merchants and banks about them.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

PCI DSS Compliance

Any merchant that takes customer payments via debit cards, credit cards or prepaid cards branded with the logo of one of the five major credit card brands is required to be PCI compliant, whether the credit card numbers are captured over the phone, in person or online. Although merchants may see the PCI DSS as a set of guidelines to quickly check off on their to-do lists, the standards exist for a more significant reason. The PCI DSS should be considered as an on-going model of best practices for merchant security and risk minimization. Businesses work hard to set forth protocol that reduces risk; the PCI DSS essentially provides all the expert guidance necessary for setting forth that protocol.

Complying with the PCI DSS should be integrated into a company's overall risk management approach. Getting everyone in the company on board and making compliance part of operations can keep it from becoming overwhelming.

The PCI Security Standards Council is not responsible for ensuring that merchants are compliant. Neither are the credit card companies. The acquiring banks, or acquirers, are accountable for merchant compliance. The acquirer is the bank or organization used by the merchant to process a transaction with a payment card. When processing a credit card transaction, the merchant requests authorization from the acquirer. The acquirer contacts the financial institution that issued the credit card to obtain approval before settling the transaction with the merchant. Because the acquirers authorize and clear the payments, they're ultimately liable, and they're the ones who issue fines. Each acquirer may hold different standards for enforcing the PCI DSS, though.

Common compliance myths

Some businesses believe that compliance simply requires a one-time solution. There's no magical answer, however, and businesses must continue to assess their risk and make changes over time. Another myth is that compliance should be relegated to the IT department. While the Technology team may be better versed in the jargon surrounding the PCI DSS, the Operations team should ensure that all employees are trained in keeping up adequate security measures. Many merchants think that compliance is too complicated and almost impossible. However, the steps necessary to achieve compliance are straightforward, and each action will only serve to improve the security and reduce the risk in a particular company. Most organizations subject to PCI regulation now use automated audit (like that available with TrueSight Automation for Servers and it's Out of the Box (OOTB) PCI content), and many use some form of automated remediation (also provided with BladeLogic's OOTB PCI Compliance Content).

The self-assessment questionnaire

The merchants that fall under levels 2-4 (more than 20,000 e-commerce or 1,000,000 non-e-commerce transactions annually) must complete the SAQ. This questionnaire includes about 250 questions that give merchants a straightforward way to evaluate whether they meet all of the

standards. Trust is placed on the merchants to accurately fill out this information. If a breach occurs, the merchant and the acquiring bank may have to pay hefty fines if the SAQ was not completed correctly. One way to ensure the Questionnaire is accurate is to use an automated Compliance engine like TrueSight Automation for Servers, with its out of the box PCI Compliance Content, to regularly (weekly or daily) audit the environment to standard, document any exceptions, and report both high-level and detailed compliance levels to leadership.

An employee of the business may complete the SAQ, but it's smart to have the SAQ completed by an expert to ensure no mistakes are made. Merchants can misconstrue language and assume they are compliant when they are in fact not. Obtaining the assistance of a PCI security expert the first time a merchant completes the SAQ can help the merchant be more confident the next time the SAQ is completed. It will help the merchant gain a comprehensive understanding of the security measures that are in effect for the business and reveal opportunities to manage security more efficiently down the road.

PCI scans

All levels of merchants may be required to undergo PCI scans conducted by an approved scanning organization. A PCI scan will uncover server and network vulnerabilities. Basically, the system that processes customers' credit card information interacts with the public, leaving it especially susceptible to attack. Because anyone can theoretically hack into the system through a merchant's website, the merchant must have a series of strong security measures set up within the system.

A PCI scan evaluates system elements, procedures and custom software to guarantee that the security controls are completely effective. PCI scans can find the holes in the network that cause a breakdown in security or allow users to bypass the safeguards. PCI scanning will test security measures such as login safety, security credentials and authentication methods. Scanning applications are able to test whether common methods used by hackers can infiltrate a merchant's system.

Although some acquirers demand quarterly PCI scans, a merchant should also run a scan any time the network is changed or updated. Network changes may include product upgrades or patches, installation of new system components, configuration change, or firewall rule modifications. BMC BladeLogic Server and Network Automation can make change detection, and validation to PCI standards easy, quick, and comprehensive across the entire PCI in-scope environment.

The PCI compliance audit

Acquiring banks may require a Report on Compliance, or RoC, which must be completed by an independent auditor, a Qualified Security Assessor. Auditors are certified by the PCI Security Standards Council and can help merchants confirm their compliance and report it to interested parties. Level 1 companies are required to submit an RoC, according to the PCI Security Standards. However, acquiring banks may require merchants of other levels to submit an RoC as well.

From the acquirer's point of view, ensuring a merchant's compliance through an RoC minimizes the acquirer's potential liability. If a merchant is not in compliance and a security breach occurs, the acquirer may be fined. From the merchant's perspective, it's probably more beneficial to be required to submit an RoC. An official PCI compliance audit can take some of the guesswork out of the compliance process and help merchants avoid misunderstandings and fines.

Consequences of non-compliance

Merchants who don't follow the PCI DSS won't get dragged to jail. In fact, the government is not in any way involved with PCI compliance. PCI compliance is not a law; it's simply a set of rules created by the e-commerce industry to support all of the players in the e-commerce industry. If a merchant has performed an assessment and come to the conclusion that it is not in compliance, the merchant is at an increased risk of security breach as well as penalty.

Penalties range from verbal warnings to fines in large dollar amounts. An acquirer may be fined up to $500,000 if a breach occurs when a merchant is not in compliance with the PCI DSS. As might be expected, that fine will typically be passed along to the merchant along with increased transaction fees. Merchants may be responsible for credit card replacement costs in the event of a breach. The merchant account agreement usually specifies the penalties for non-compliance, but they are significant enough that organizations cannot ignore them.

If a merchant is frequently found to be violating the rules, that merchant may lose the privilege to accept payment cards altogether. This can, obviously, be a death sentence for a business. Merchants who lose their payment processing accounts are often unable to open another account for years, losing credibility and customer loyalty and making it almost impossible to do business.

Evaluating vulnerability

If a merchant is not in compliance with the PCI DSS, it is necessary to evaluate which areas need work and which are a higher priority. The most vulnerable security risks should be addressed first. For example, a weakness that leaves customer information open to attack must be repaired before looking at compliance involving proper documentation.

If the credit card processing system can be extracted from other systems, PCI security measures only need to be applied to the card transaction system. That can reduce the amount of resources a company needs to maintain compliance and create security controls.

A third party can help companies evaluate their vulnerability and establish adequate security measures to manage PCI compliance. Using a third party to test security controls can help a business be more efficient and focus on what it does best, which is providing a service or product to the community.

Ensuring compliance through a third-party service provider

Some merchants use third parties to process online payments. These payment processors may provide the merchant with a secure checkout page that appears to be part of the merchant's website but really stores and processes all data on the service provider's side. Using a service provider can minimize the merchant's risk of experiencing security issues, but it does not eliminate the merchant from PCI compliance. Merchants who use a third-party service provider should still have their systems assessed by a professional to make sure there are no potential security issues on their end.

PCI compliance levels

Regardless of the compliance level that classifies them, businesses must comply with all of the PCI standards, but the level of compliance will denote the type of reporting the merchant must submit

to the acquirer. Below is an explanation of the different PCI compliance levels.

Level 4
Small businesses that process fewer than 20,000 transactions through their websites and fewer than 1 million non-ecommerce transactions annually must complete a self-assessment questionnaire, or SAQ, every year. Level 4 merchants may also be required to undergo quarterly PCI scans.

Level 3
Companies that process between 20,000 and 1 million transactions must follow the same reporting requirements as level 4 merchants.

Level 2
Level 2 merchants process between 1 million and 6 million transactions each year. These companies must also fill out an SAQ and may have to undergo quarterly PCI scans.

Level 1
The largest companies, those that process upwards of 6 million transactions per year, may be required to have quarterly PCI scans administered. Level 1 companies must undergo an annual PCI audit as well.

Creating a PCI compliance Checklist

Filling out the SAQ with a PCI security professional can help merchants create a checklist of necessary safeguards to implement and maintain. A PCI compliance checklist may include a number of common security best practices:

- Customizing system passwords and changing them regularly;
- Creating and sustaining firewall protection;
- Encrypting transmission of private data across networks;
- Upholding a vulnerability management program that involves regular patch deployment, configuration management, and using and updating anti-virus software;
- Restricting access to company data; and
- Creating a policy to address information security

Any business that handles credit card transactions is required to comply with the PCI DSS. Even the simplest home-based businesses are vulnerable to attack because personal computers often have long open broadband connections and fewer security measures. According to a recent report, Americans are more afraid of credit card data fraud and identity theft than anything else, including personal safety and terrorism. Understanding the PCI DSS can help merchants establish credibility with their clients, create confidence in their security and limit the risk involved with processing private customer information on a daily basis.