

AUXIS™



PCI DSS Compliance: Failure is not an option

Published: November 2008

Every company that accepts credit card payments, processes credit card transactions, stores credit card data, or in any other way touches personal or sensitive data associated with credit card payment processing is affected by PCI DSS (Payment Card Industry Data Security Standards).

Credit Card Fraud Risk

The use of online retail services to make it easier for customers to purchase goods and services has grown exponentially in recent years. In order to facilitate the purchasing experience for the customer, online retailers provide a mechanism whereby customers pay for the goods or services online by credit or debit card. This improved efficiency and convenience for the consumer has also unfortunately provided a significant opportunity for criminals to gain access to consumer credit data to commit fraudulent activities. Due to the significant amount of money that can be acquired with very little risks, criminals have concentrated their efforts on both accessing the credit card repositories and capturing credit card transactions. Credit card fraud is the single most common form of identity theft reported. Credit cards also represented the majority of the \$315 billion US financial fraud loss reported in 2005 (Source: *International Herald Tribune*). High profile cases have hit the headlines such as the TJ Stores (TJX) security breach in which over 100 million credit and debit card numbers were stolen by hackers who were able to penetrate the network over a period of at least 18 months.

According to *Internetnews.com* the latest estimate of TJX expenses related to the breach is between \$500 million to \$1 billion, this estimate does not include damages to company image and reputation.

In addition to the loss from fraudulent transactions, banks and other organizations also incur high administrative costs associated to the breach such as losses to replace compromised cards and lost interest and transaction fees. In an effort to reduce the risk of fraud and improve consumer confidence in online retailing, the major retail electronic payment networks (Visa, MasterCard, American Express, Discover, JCB) created the Payment Card Industry Data Security Standard (PCI DSS), which outlines general security requirements for companies that store, process, or transmit cardholder data.

About PCI DSS

To promote PCI DSS compliance and reduce the fraud risks, the electronic payment networks began enforcing compliance requirements on all companies that perform online credit card transactions. Some card brands have threatened either huge fines against merchants of up to \$25,000 per month until compliance is obtained or the possibility of having their merchant status revoked and potentially being banned from accepting or processing credit cards.

By following the standardized, industry-wide procedures of PCI DSS, your organization can reap the following benefits:

- Protect your customers' personal data including credit card information when used to make a single or recurring payments
 - Boost customer confidence, and safeguard the reputation of your brand through a higher level of data security
 - Protect your business from financial penalties. One of the benefits of PCI DSS compliance is that the organization will not face a severe penalty if their services are breached. If the analysis after a security incident shows that the company was still compliant at the time of the incident, this will result in more lenient treatment by the authorities
 - Obtain lower credit card processing cost structure and lower per-transaction processing fees from the credit card companies
 - Potentially be eligible to receive part of \$20 million in financial incentives from Visa if your company is a Level 1 or Level 2 merchant
 - Have increased confidence that your organization has less chance of occurrence of fraud because it has been proven that merchants who comply with PCI DSS have a lower rate of fraud and lowered losses to fraud.
 - Be protected from unwanted negative media attention
- Leverage the effort to implement PCI DSS compliance for other regulatory compliance requirements such as SAS-70 and Sarbanes-Oxley.

To comply with PCI DSS your organization must meet 12 requirements that in summary address the following six business and technology issues:

- Building and maintaining a secure network
- Protecting cardholder data
- Maintaining a vulnerability management program
- Implementing strong access controls
- Regularly monitoring and testing networks
- Maintaining an information security policy

The PCI standard requires continuous validation of security efforts, so companies complying with PCI DSS must create a framework for governance and change control of policies and procedures that provides a mechanism to ensure compliance throughout the period and can be leveraged for future audits. Experience has shown that PCI DSS compliance is most successful when the related business processes are included in-scope. Instead of focusing solely on acquiring technology-based solutions (detection systems, firewalls, software, etc) organizations have found that by re-aligning the underlying procedures that manage how data is processed they have been either able to achieve compliance or been able to better define functional requirements to purchase the best-fit technology solution.

A Well Balanced Approach to Compliance

PCI DSS compliance can initially seem like an overwhelming task. The key to being successful with this type of compliance project (or any other type of compliance project) rests in a well balance approach to the project. This approach is outlined in the following steps:

1. **Assemble the correct team** – The team needs to have the right blend of business and technical resources. The business resources provide the understanding and knowledge of the business process used to process the transactions. The technical resources will provide the ability to test the underlying systems/applications supporting the key business processes.
2. **Develop a project charter and plan** – The key to any successful project is to develop a charter that is specific to the project and to obtain buy-in from all the parties concerned. This is does not just include the project team, but also includes the various individuals and departments in the organization that are involved with the key business processes. The next step is to build a project plan with checkpoints that will allow the team to stay on track.
3. **Develop a tracking mechanism** - The project team will need to develop a mechanism to track progress, resolve issues and present deliverables. A central repository and a compliance management solution are two tools that will help the team achieve these goals.
4. **Demonstrate compliance** – a properly developed compliance management solution will facilitate the main objective of the project – being able to show PCI DSS compliance to both senior management and to external auditors/stakeholders.



About Auxis:

Auxis is a leading Management Consulting firm headquartered in Coral Gables, Florida. Our methodology is designed to provide our clients with real-world business solutions, anchored by solid financial analysis. Auxis can help you to attain PCI DSS compliance through service offerings such as strategic evaluation, provider selection and deployment, and IT supporting infrastructure, selection, and deployment.

Auxis' deep experience and proven methodology has navigated many organizations various compliance projects. Compliance requirements can represent a significant opportunity for the business. Selecting the right provider (the "Who") for the appropriate functions (the "What") in the right areas (the "Where") at the right time (the "When") for the right reasons (the "Why") are the keys to a successful compliance project. All of the factors should be well understood by the key stakeholders in the business. The right selection can result in significant financial and efficiency gains for the business, but the wrong selection can be disastrous. If you have a compliance project, contact Auxis for our expert guidance and support.

Headquarters

55 Miracle Mile, Suite 300
Miami, Florida 33134
(305) 442-0060

www.auxis.com

Ft. Lauderdale

7901 SW 6th Court, Suite 130
Ft. Lauderdale, Florida 33324
(954) 236-6682

Atlanta

3500 Lenox Road, Suite 300
Atlanta, GA 30326
(404) 419-2215

Washington, D.C.

1701 Pennsylvania Ave, Suite 300
Washington, D.C. 20006
(202) 390-8606