PCI DSS Compliance Overview

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard defined by the Payment Card Industry Security Standards Council. The standard was created to help protect organizations that process card payments from credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations that hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands.

PCI Compliance is a requirement mandated by the payment card industry, that protects organizations and their clients from fraud. This allows organizations to maintain the trust of their customers and stay in business.

Typical Path to PCI DSS Compliance

All companies and organizations that deal with credit card information must adhere to PCI DSS, including organizations that take credit card payments online, in person, or via a call center.

Here are the basic goals the PCI DSS tries to achieve:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

PCI DSS SAQ A Compliance

SAQ A is for card-not-present companies who outsource all functions related to collecting, storing and exchanging the credit card data to a third-party validated PCI company. This means that the companies never come in contact with the cardholder data and that the data never enters their company's environment.

To be eligible for SAQ A, e-commerce merchants must meet eligibility criteria, including that there are no programs or application code that capture payment information on the merchant website. Examples of e-commerce implementations that fall under SAQ A include:

- Merchant has no access to their website, and the website is entirely hosted and managed by a compliant third-party payment processor
- Merchant website provides an inline frame (iFrame) to a PCI DSS compliant third-party processor facilitating the payment process
- Merchant website contains a URL link redirecting user from merchant website to a PCI DSS compliant third-party processor facilitating the payment process

The table below summarizes the SAQ A requirements:

	SAQ A All Cardholder Data Functions Completely Outsourced
Applies to	**Card-not-present** merchants (e-commerce or mail/telephone-order)
Functions Outsourced	**All processing** of cardholder data is entirely outsourced to PCI DSS validated third-party service providers
Payment Pages	All elements of all payment pages delivered to the consumer's browser **originate only and directly** from a PCI DSS validated third-party service provider(s)
Third-Party Compliance	Merchant confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant
Merchant Systems	Merchant does not electronically store, process, or transmit any cardholder data on their systems or premises, but relies entirely on a third party(s) to handle all these functions
Data Retention	Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically

StratusWorX outsources all processing of cardholder data to PCI DSS validated third-party service providers, including PayPal, Western Union Speedpay and Visa Authorize.net. Further, StratusWorX provides an iFrame to the PCI DSS compliant third-party processor to facilitate the payment process. By removing the responsibility of credit card processing, exchanging and storing from the organization, StratusWorX becomes eligible for SEQ A certification in order to achieve full PCI DSS compliance.

For more information about PCI DSS Compliance and to view the comprehensive SAQ A Questionnaire, visit www.pcisecuritystandards.org.