

Payment Card Industry (PCI)

Data Security Standard Certification Services



Introduction

Over the past few years, online crime and theft involving credit card data has become big business for cyber criminals. Numerous stories involving the compromise of hundreds of thousands of credit cards have emerged, resulting in millions of dollars in losses to both card issuers and consumers. To ensure that cardholder data is protected, the Payment Card industry has created the PCI Data Security Standard (PCI DSS). Failure to comply with the PCI DSS can result in losing the ability to process credit card payments, and could also result in severe financial penalties.

SRS provides with its Security Services for PCI a comprehensive set of services to assist banks, processors, payment service providers and merchants in achieving compliance with the PCI DSS requirements. The proven PCI DSS methodology and rendering of services are separated into different stages to assist our clients in achieving compliance. During these stages, SRS provides the client with mandatory and optional services to allow the customer to achieve compliance in an efficient and timely manner. These stages are:

Education and Assessment Preparation

To understand the focus of PCI DSS and to define the scope of relevant areas SRS provides in this stage detailed information and training to the client to improve the level of attention and understanding of the management and involved staff members.

Compliance Advisory and Support

During this stage the identification of weaknesses and deviations from the requirements of the PCI DSS is performed. For clients, who have not undergone a PCI validation in the past, SRS recommends this phase or parts of this phase to highlight areas of non-compliance and prioritize the respective remediation activities.

Vulnerability Scanning Services

The PCI DSS requires that vulnerability scans are performed on a regular basis. The scan detects vulnerabilities on the external facing IP addresses of the clients' network infrastructures to help in identifying gaps and to improve the external security.

Assessment Services

An onsite review according to the PCI Security Audit Procedures is conducted by ControlCase auditors together with the responsible staff of the client during an onsite visit. This review address processes and procedures, physical and logical security, documentation, and security management.

The PCI Security Standard

The Payment Card Industry Data Security Standard [PCI DSS] is a set of comprehensive requirements for enhancing payment account data security. The PCI DSS was jointly developed by Visa International, MasterCard, American Express, JCB and Discover several years ago. In 2006 the PCI Security Standard Council [PCI SSC] was founded by these card organisations to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations for proactively protect customer account data.

Structure of the Standard

The PCI DSS is a group of principles and accompanying requirements, grouped in six main sections addressing more than 300 single requirements. The six main sections are:

Build and Maintain a Secure Network

Protect Cardholder Data

Maintain a Program f. Vulnerability Mgmt.

Strong Access Control Measures

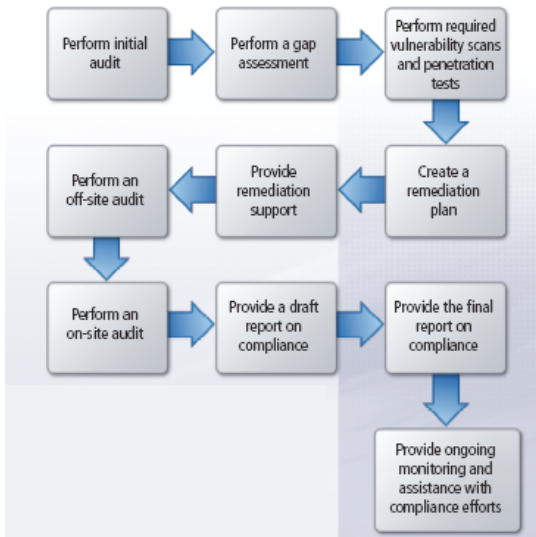
Monitor and Test Networks

Maintain Information Security Policy





Process and Deliverables



The process is designed to ensure that organisations can take their card services into a secure framework. The PCI DSS standard is openly available at <https://www.pcisecuritystandards.org/> and enables organisations to assess their state of maturity before a certification audit is carried out.

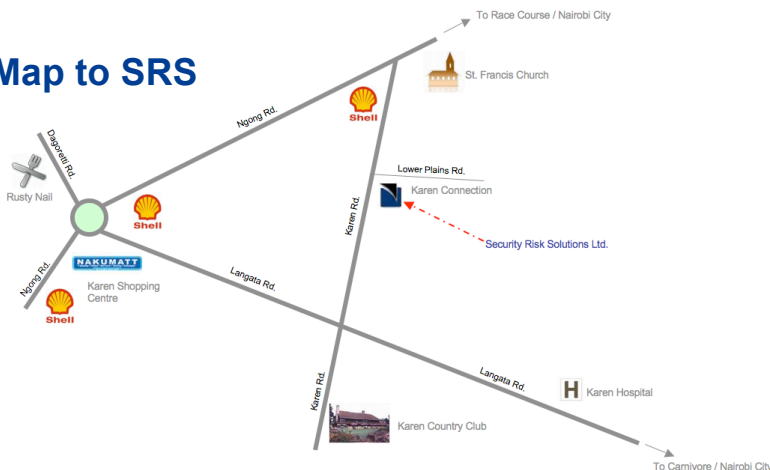
Certification Process:

- a) Initial Audit and Gap Analysis is carried out by card organisation or SRS
- b) Security Testing is carried out by card organisation, third party or SRS
- c) Card organisation implements a Remediation plan to meet criteria
- d) After all criteria are met, ControlCase performs formal certification Audit (1-2 weeks)
- d) ControlCase issues audit report and awards Certificate



To receive a quotation for secure online certification services, please contact one of our leaders below.

Map to SRS



Key Contacts

- Kostja Reim (Information Security)
Nairobi
+254 (020) 883312/3
kostja.reim@securityrisksolutions.net
- Jason Finlayson (Business Continuity)
Nairobi
+254 (020) 883312/3
jason.finlayson@securityrisksolutions.net
- Andy Townsend (Computer Forensics)
Nairobi
+254 (020) 2019286
andy.townsend@securityrisksolutions.net