

# PCI Gap Analysis and Remediation Planning



## Expertise You Can Trust

Compliance with the PCI Data Security Standard (PCI DSS) is vital to all merchants who store, process or transmit credit cards, because nothing is more important than keeping your customer's payment card data secure. Becoming PCI compliant is not a simple matter of updating passwords, or cobbling together a technology solution. It requires a much more comprehensive set of technologies and processes designed to manage the risks associated with credit card fraud. More than just technology and tasks, PCI compliance requires an in-depth security program to manage risks.

Reliant Security is a market leader in Payment Card Industry Data Security Standard (PCI DSS) compliance technology solutions for retail merchants. Our products and services help our clients meet the PCI DSS control objectives. Reliant Security has been working with merchants for years, helping them develop a strategic and comprehensive data security program. Our in-depth expertise in retail and network technology, and PCI DSS requirements enables us to deliver on these objectives. Our team is CISSP and QSA certified, and Reliant is an active member of the PCI Security Council.

## Gap Analysis Overview

The PCI Standard consists of what have come to be known as the "Digital Dozen" requirements for protecting credit card information. Each of these top-level requirements consist of a number of sub-requirements found at: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org). Reliant Security will review the client's IT environment specifically as it relates to each component of the "Digital Dozen" and cardholder data. The result of our analysis will provide the assessment, road map and recommendations to ensure your retail environment meets the PCI requirements. Our professional consulting services include analysis and assessment in identifying and preventing threats to your retail environment. The scope of the analysis may include corporate offices, store locations, e-commerce and catalog environments. We will assess your information security posture, and gaps in compliance. The network infrastructure, system components, POS and other card processing applications, business processes and operational personnel supporting the management of cardholder data are also evaluated.

Based on the evaluation, Reliant will provide a Cardholder Data Environment Characterization. This document will include detailed dataflow diagrams illustrating how business processes store, process and transmit sensitive payment card data. In addition to detailing processes, Reliant will document relevant details associated with the technology environment used to process card data. Once the environment that stores, processes and transmits sensitive cardholder data is defined, gaps can be properly assessed.

A gap analysis will include documentation review, on-site evaluations, and network vulnerability scans. To begin the process, Reliant Security will review client security policies, standards, and configuration guidelines. These documents are used to provide a detailed assessment of the client's PCI compliance posture.



PCI COMPLIANCE SIMPLIFIED

# PCI Gap Analysis and Remediation Planning



Based on this, Reliant will provide remediation planning. Remediation planning deliverables range from a high-level road map which illustrates tasks and time frame required for PCI compliance to very detailed control design documents. Reliant's PCI Remediation services include:

- Security Program Development
- Card Processing Architecture
- Technical Controls Design
- Policies and Procedures

## PCI Assessment Deliverables

1. Scope of the assessment specifying systems investigated, number of sites visited, number of network components scanned and/or evaluated.
2. Dataflow diagrams for all identified payment applications and processes.
3. Analysis of vulnerabilities including prioritization of security issues based on threat likelihood and economic impact across retail and headquarters environments.
4. Analysis of key compliance gaps between current information security state and PCI requirements across headquarters, store locations, and eCommerce environments.
5. Remediation road map, which outlines critical remediation projects and IT controls that will be required to close compliance gaps.

## Innovation & Expertise

Reliant Security has a proven track record of innovation in data security and compliance. Reliant was the first solutions provider to deliver a comprehensive security appliance for merchants with distributed locations that satisfies each of the PCI DSS technical controls. The MPS Redbox is Reliant Security's flagship security appliance, designed to provide broad, integrated, and high-performance protection against data security threats, while simplifying and reducing the costs of PCI remediation.

You can trust Reliant Security to deliver an accurate PCI Assessment and industry-leading security solutions for your business.

## Visa PCI "Digital Dozen" top-level requirements

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security



450 7th Avenue, Suite 503 • New York, NY 10123 • 917-338-2200  
[www.reliantsecurity.com](http://www.reliantsecurity.com)

PCI COMPLIANCE SIMPLIFIED