



CONSULTING SERVICES: Security & Compliance

Compliance with the Payment Card Industry Data Security Standard (PCI DSS) is vital to all merchants that store, process or transmit credit cards, because nothing is more important than keeping your customers' 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 is a market leader in PCI DSS compliance technology solutions for retail merchants and is an active Participating Organization in the PCI Security Standards Council. We are currently a Level 1 Certified PCI Service Provider and were the first company to attain Qualified Integrator and Reseller ("QIR") status under the PCI Security Standards Council's QIR program. Our products and services help our clients meet the PCI DSS control objectives.

Solutions-Oriented Approach to PCI Compliance

For years, Reliant has helped merchants develop comprehensive data security programs that comply with PCI DSS requirements. Our approach to PCI DSS compliance is focused on achieving reliable, scalable and cost-effective solutions to secure payment card transactions and meet challenging PCI DSS compliance requirements. This includes the design and implementation of payment technology solutions as well as development of processes for Security Operations and IT Governance.

VISA PCI "DIGITAL DOZEN"

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





CONSULTING SERVICES: Security & Compliance

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 consists of a number of sub-requirements, which can be found at www.PCIsecuritystandards.org. Reliant reviews our clients’ IT environment specifically as it relates to each component of the transaction processing path and PCI DSS requirements. The result of our analysis will provide the assessment, road map and recommendations for security and compliance.

Based on the evaluation, Reliant provides a Cardholder Data Environment Characterization. This document includes detailed dataflow diagrams illustrating how business processes store, process and transmit sensitive payment card data. In addition to detailing processes, Reliant documents relevant details associated with the technology environment. Once the payment card environment is defined, PCI DSS compliance gaps are properly assessed.

Based on this, Reliant provides remediation planning solutions that range from a high-level road map illustrating tasks and time frames required for PCI compliance, to payment system and technical control design and implementation. All Payment Application deployments meet PCI QIR Program Requirements adding an additional layer of oversight from the PCI Council to ensure that critical payment system design and implementation efforts conform to PCI DSS Standards.

Reliant’s PCI Remediation services include:

- Card Processing Penetration Test and Vulnerability Analysis
- Payment Card Processing Architecture
- Security Program Development
- Payment System Design and Implementation
- Security Controls Design and Implementation
- Policies, Procedures and Standards

Proven Innovation & Expertise

Reliant 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. We were also the first company to attain Qualified Integrator status under the PCI Security Standards Council’s QIR program. Redbox Platform, Reliant’s flagship patented security appliance, is designed to provide broad, integrated and high-performance protection against data security threats, while simplifying and reducing the costs of PCI remediation.

About Reliant

Reliant’s Redbox Platform transforms the delivery and support of retail systems through an appliance-based converged infrastructure solution, which enables a wide range of application, systems and network configurations. The Redbox Platform solution replaces Retail’s traditional, inflexible approach to store systems with an agile model that can be centrally managed across a countless number of stores and eliminates the need for additional dedicated equipment to run each in-store application. The result: retail executives can keep pace with 21st century customer-engaging applications while keeping costs in control by using this highly flexible and secure architecture.

