



Payment Card Industry (PCI) Data Security Standard (DSS) Motorola PCI Planning and Assessment





Retail establishments have always been a favorite target of thieves and shoplifters, but today's most insidious criminals never even enter the store. They can be out on the sidewalk or even thousands of miles away on a different continent, utilizing the Internet and wireless connections to gain access to your most precious assets – your customer records and payment card numbers. The Payment Card Industry (PCI) Data Security Standard (DSS) is a worldwide mandate designed to protect retail customers' records and payment card numbers from unauthorized access. The cost of non-compliance is high – measured in high fines, the high cost of consumer lawsuits and brand damage. Achieve compliance and protect your customers, as well as your profitability with Motorola's PCI Planning and Assessment Service.

Retailers under attack

Retail establishments have always been a favorite target of thieves and shoplifters, but today you can't even see them coming. Today's most insidious criminals never even enter the store. They can be out on the sidewalk, sitting in a parked car, in a hotel room across town, or even thousands of miles away on a different continent. They work through the Internet or through wireless connections to gain access to your most precious assets – your customer records and payment card numbers.

Their actions can devastate your business, your reputation, and your customers — and it can cost you and the credit card companies millions of dollars. It has been estimated that the major security breach of a well-known US retailer will cost the company anywhere from \$1 billion to more than \$4 billion. And there is no end in sight.

What is it all about?

PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

The PCI DSS consists of six high-level goals and twelve core requirements (see chart 1) that apply to all enterprise, small and mid-sized business (SMB), service providers and retail organizations that handle (store, process or transmit) credit card transactions. The PCI DSS also specifies the need for quarterly and annual security assessments and audits to prove compliance with these standards.

The cost of not complying

Failure to comply with the PCI DSS can be expensive. A Level 1 merchant, for example, can be charged \$25,000 for each month that they are out of compliance. Moreover, failure to comply with the PCI DSS can result in the merchant being prohibited from accepting credit cards. Other costs of non-compliance could include:

- Shareholder and consumer lawsuits
- Damage to brand reputation (resulting in a loss of both clients and credibility)
- Fines for level 1 and level 2 merchants per month of non-compliant status

Chart 1

Achieving PCI Compliance: six goals, twelve requirements

Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need-to-know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for employees and contractors



- Merchant fines of \$100 to \$1,000 per transaction if a full card number is stored or printed on a customer receipt

What are the compliance deadlines?

The global PCI Security Standards Council, the independent body set up to govern card providers and merchants, among others, stated that by 1 October 2008, all merchants — regardless of their levels — must be PCI DSS compliant.

In November 2008, VISA announced worldwide mandates for PCI DSS compliance:

- September 30, 2009: Companies cannot store "Prohibited Data." This includes: magnetic stripe or track data, card verification value or code data, PIN or PIN block data even if encrypted.
- September 20, 2010: Level 1 merchants must be fully PCI compliant with each of the 280 points being satisfied. If they are found to be non-compliant they will be fined.

Motorola's PCI Planning and Assessment Service

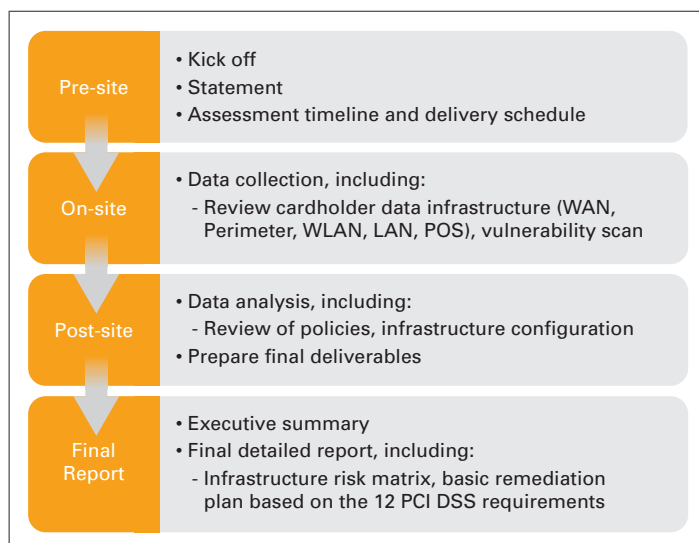
Motorola's PCI Planning and Assessment Service helps you prepare for PCI compliance audits by assessing your cardholder data infrastructure against the PCI DSS requirements. We conduct a thorough review of your security processes and policies, perform network vulnerability scans, and analyze your network architecture

to uncover any gaps that may exist. If gaps are found, we provide a full report including specific recommendations and action plans for closing them.

This Motorola service:

- Identifies the cardholder data environment within your network
- Executes automated security assessment tools as needed on in-scope hosts
- Evaluates technical controls
- Reviews and analyzes network architecture
- Performs WLAN site-survey focusing on rogue access point (AP) detection and use of non-compliant WLAN technology
- Reviews operation controls and documentation
- Conducts personnel interviews to understand policy and procedures
- Maps requirements to controls to demonstrate evidence of executing those controls
- Identifies PCI DSS gaps and provides gap closure recommendations

Our Methodology



Benefits of Motorola's PCI Planning and Assessment

Motorola's PCI Planning and Assessment Service allows you to:

- Satisfy PCI DSS compliance requirements
- Be well prepared for the onsite PCI QSA Audit, reducing the time required for the whole process
- Expose high security threats within your cardholder data infrastructure and implement a remediation plan
- Prioritize IT investment planning and PCI DSS compensating controls, based on assessment analysis (protect your business critical processes and data first)

The Motorola Security Services Team

Motorola's PCI Planning and Assessment Service is delivered by Motorola Security Services, a team of highly certified security professionals (CISM, CISA, CISSP, CEH, former PCI QSAs) with deep experience in network and application security, wireless security, all areas of networking, and PCI DSS compliance.

As leaders in network security, these specialists stay on top of the rapidly changing landscape of security threats and compliance technologies, and continually refine their tools and skills to help guide you through your PCI and other compliance needs. Through years of working with companies, service providers, and government customers, Motorola Security Services has developed a strategy based on a proven approach and methodology that encompasses people, processes, policy and technology. We go beyond typical security controls to help you succeed in protecting your network and information.

Why Motorola?

Motorola is a world leader and trusted partner in wireless network solutions. From WiFi to WiMAX, cellular to mesh, few companies can match our history of wireless insight and innovation.

Motorola was also one of the first companies to recognize the threat of Internet crime and wireless breaches. We also developed many of the processes and procedures that became the core of many companies' security posture.

We are using well known Information Security best practices and methodologies (Cobit 4.1, CIS Benchmarks, ITAF, ITIL v2/3 Security Management, NIST, NSA IAM, OCTAVE, SANS, ValIT) to satisfy international/national Information Technology standards such as PCI DSS, German BDSG, Data Protection Act(s), EU Directive 95/46/EC, GLBA, HIPAA, ISO 17799/27001/27002, and SOX/Euro-SOX.

Finally, as a recognized security thought leader and wireless technology innovator, we accepted the invitation to join the Payment Card Industry Data Security Standards Board and help define the retail security standards.

For more information

For additional information about Motorola Security Services, please contact your local Motorola representative or

- *Visit us on the Web at www.motorola.com/business/services*
- *Access our global contact directory at www.motorola.com/enterprisemobility/contactus*



MOTOROLA

motorola.com

Part number SVCS-PCIDSS-NALA. Printed in USA 05/09. MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. ©2009 Motorola, Inc. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.