Ensuring Compliance With PCI STANDARDS

With the recent rise in data breaches of credit card information and rising identity thefts, not implementing a sound information security program is no longer an option.

Companies processing credit card information must embrace and implement sound data protection strategies to ensure the confidentiality and integrity of the customer's payment information. The cost of compliance, while significant, is far less expensive than the cost of remediation, where public out-cry and media coverage of a breach could damage a company's brand irreparably.

To counter this enormous problem and protect customers' credit card data, the five major credit card companies—Discover, American Express, Visa, MasterCard and JCB—teamed up to form the Payment Card Industry (PCI) Security Standards Council. As outlined by the council, any transaction or account information is required to be confidential and safe from hackers or other intruders. To enforce these requirements, the PCI Security Standards Council has mandated that all merchants and service providers who store, process or transmit payment card information need to be PCI compliant. Penalties for noncompliance include monetary fines, and/or account suspension and termination.

Learn how Mainline Payment Card Industry solutions can secure your cardholder data

With a broad product and service portfolio, industry expertise and a deep understanding of PCI requirements, Mainline delivers the level of support organizations need to achieve and maintain PCI compliance. With its combined solutions, Mainline helps companies evaluate their overall security posture, and implement proper controls and security technology, to meet the PCI data security standards (DSS).

As part of a layered security model that includes cost-effective encryption, versatile authentication and e-mail security solutions, Mainline is committed to helping merchants and service providers of all sizes protect their customer data and manage compliancy issues associated with these PCI data security requirements.

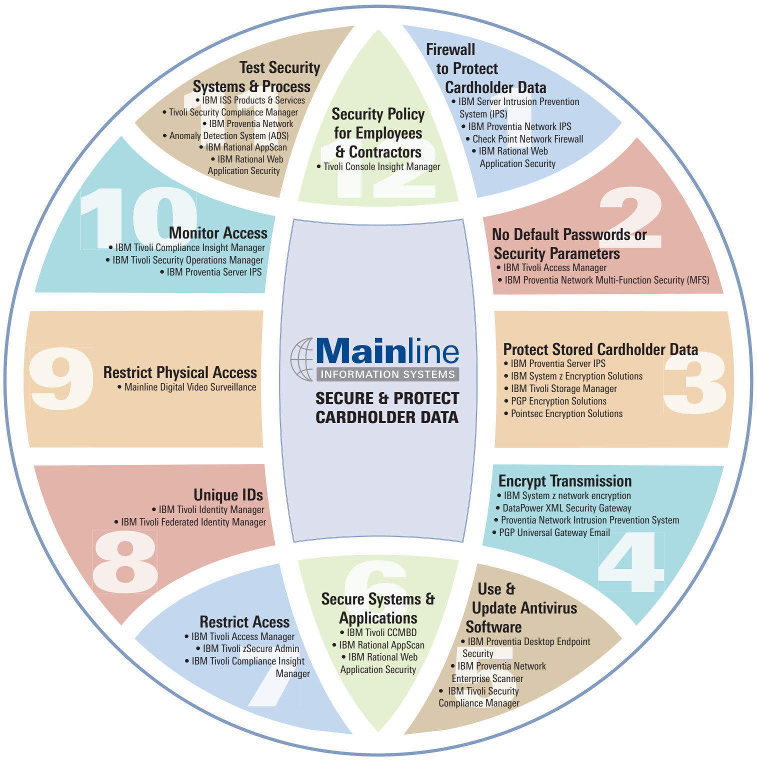
The 12 requirements as defined by the Payment Card Industry Security Standards Council

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder 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.

Visa and MasterCard merchant levels and compliance requirements

LEVEL	DESCRIPTION	REQUIREMENT	VALIDATED BY
1	Visa U.S.A. and MasterCard World Wide transactions totaling 6 million and up, per year, and any merchants who experienced a data breach.	• Annual On-site PCI Data Security Assessment • Quarterly Network Scan	• Qualified Security Assessor or Internal Audit, if signed by Officer of the company • Approved Scanning Vendor
2	Visa and MasterCard transactions totaling 1 million to 6 million per year.	• Annual PCI Self-Assessment Questionnaire • Quarterly Network Scan	• Merchant • Approved Scanning Vendor
3	Visa and MasterCard e-commerce transactions totaling 20,000 to 1 million per year.	• Annual PCI Self-Assessment Questionnaire • Quarterly Network Scan	• Merchant • Approved Scanning Vendor
4	Visa and MasterCard e-commerce transactions totaling up to 20,000 per year.	• Annual PCI Self-Assessment Questionnaire • Quarterly Network Scan	• Merchant • Approved Scanning Vendor

Ensuring Compliance With PCI STANDARDS



Mainline INFORMATION SYSTEMS
SECURE & PROTECT CARDHOLDER DATA

1 Firewall to Protect Cardholder Data
- IBM Server Intrusion Prevention System (IPS)
- IBM Proventia Network IPS
- Check Point Network Firewall
- IBM Rational Web Application Security

2 No Default Passwords or Security Parameters
- IBM Tivoli Access Manager
- IBM Proventia Network Multi-Function Security (MFS)

3 Protect Stored Cardholder Data
- IBM Proventia Server IPS
- IBM System z Encryption Solutions
- IBM Tivoli Storage Manager
- PGP Encryption Solutions
- Pointsec Encryption Solutions

4 Encrypt Transmission
- IBM System z network encryption
- DataPower XML Security Gateway
- Proventia Network Intrusion Prevention System
- PGP Universal Gateway Email

5 Use & Update Antivirus Software
- IBM Proventia Desktop Endpoint Security
- IBM Proventia Network Enterprise Scanner
- IBM Tivoli Security Compliance Manager

6 Secure Systems & Applications
- IBM Tivoli CCMBD
- IBM Rational AppScan
- IBM Rational Web Application Security

7 Restrict Acess
- IBM Tivoli Access Manager
- IBM Tivoli zSecure Admin
- IBM Tivoli Compliance Insight Manager

8 Unique IDs
- IBM Tivoli Identity Manager
- IBM Tivoli Federated Identity Manager

9 Restrict Physical Access
- Mainline Digital Video Surveillance

10 Monitor Access
- IBM Tivoli Compliance Insight Manager
- IBM Tivoli Security Operations Manager
- IBM Proventia Server IPS

11 Test Security Systems & Process
- IBM ISS Products & Services
- Tivoli Security Compliance Manager
- IBM Proventia Network
- Anomaly Detection System (ADS)
- IBM Rational AppScan
- IBM Rational Web Application Security

12 Security Policy for Employees & Contractors
- Tivoli Console Insight Manager

The Mainline PCI Compliance Program

As the logical first step to compliance, the Mainline PCI assessment offering is comprised of the following services:

Annual onsite PCI assessment with report on compliance (ROC) – provides a comprehensive evaluation of the organization's information security program, according to PCI specifications for networks, servers and databases involved in the transmission, storage and processing of credit card data.

Quarterly scanning services – includes a vulnerability assessment to help ensure and validate that proper security precautions are in place.

Pre-assessment – a customized gap assessment determines the current level of compliance and outlines the specific steps required to effectively achieve PCI DSS compliance before performing the formal assessment.

Penetration testing – demonstrates a real-life network attack to determine current vulnerabilities and analyze how attackers significantly impact a business.

What Makes Mainline Your Trusted Partner for Information Security

Mainline believes that the key attributes of a credible Information Security partner are experience, certifications and longevity. These qualities distinguish Mainline as a trusted Information Security partner for leading organizations.

Experience

The combined experience of our Information Security team spans over 100 years, and reflects expertise in all segments of the security industry. We work with clients that include many of America's largest organizations and government agencies, and we provide services to major clients throughout Mexico and Puerto Rico.

Certifications

Mainline ensures that the experience of its Information Security team is backed by independent assessments and certifications. Mainline employs some of the most respected security experts in the field, bringing a wealth of experience to deal with the security issues you face today. Our expertise ranges from experienced security sales consultants to security-certified technical engineers. By applying expertise in security, networking, operating environments and storage technologies, as well as our unique skills in consulting, integration and managed services, we are able to create customized security solutions for our clients.

Longevity

When you select an Information Security solution, you want a lasting partnership. Backed by 25 years of IT experience, Mainline is a nationally recognized solution provider helping clients develop and implement the right solutions to solve business needs.

MAINLINE....YOUR INFORMATION SECURITY PARTNER

* Best-of-breed solutions for all your security needs
* Highly skilled and certified security practitioners
* Trusted security advisor and partner
* Sales and technical resources throughout the country
* Award-winning company

For more information on Mainline's information security solutions, please call **1.866.490.MAIN(6246)**, or visit **www.mainline.com**.