

TraceSecurity Compliance Manager™ PCI

KEY BENEFITS

- Ensure compliance with PCI Data Security Standard
- Enforce a policy of continuous risk management
- Achieve a constantly verifiable security posture

PCI REQUIREMENTS OVERVIEW:

Build and Maintain A Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain An Information Security Policy

Requirement 12: Maintain a policy that addresses information security

PCI Defined The Payment Card Industry (PCI) Data Security Standard (PCI DSS) requires businesses to protect credit cardholder information.

It is a contractual agreement that outlines a private technical standard for how sensitive data is handled. It is a service requirement that the credit card companies provide to merchants. All merchants and service providers who handle, transmit, store, or process information concerning any of these cards, or related card data, are required to be compliant with PCI. Fulfilling the contractual obligation involves a process of verifying compliance by following a set of IT procedures that range from standard configurations, best practices, change management procedures, and validation.

Penalties

As of September 30, 2007, a merchant may be fined up to \$100,000 per month if they are not compliant with PCI DSS. If there is an incident of data compromise, the fines may reach up to \$500,000 per incident. In addition, noncompliant merchants may be banned from performing credit card transactions.

Acquiring banks that fail to ensure compliance by September 30, 2007 will be assessed fines starting at \$5,000 a month for each noncompliant merchant. The fines increase to \$25,000 per month after December 31, 2007.

How We Help

TraceSecurity is an approved PCI DSS scanning vendor, and is fully certified to assess PCI DSS compliance. We provide a highly-automated, cost-effective way for organizations to achieve PCI compliance.

Our solution, TraceSecurity Compliance Manager PCI, automates the process of PCI compliance. Delivered as an on-demand service over the web, Compliance Manager PCI provides PCI compliance testing and reporting. Compliance Manager PCI also provides an easy-to-use interface which enables merchants and member service providers to complete the PCI self-assessment questionnaire and conduct security scans to efficiently identify and eliminate security vulnerabilities.

Validation Requirements Based on Transaction Volume and Business Type

The table below is a representative sample of the requirements from MasterCard and VISA.

	ON-SITE AUDIT	SELF-ASSESSMENT	NETWORK SCAN
MERCHANTS			
Level 1 Any merchant – regardless of acceptance channel – processing over 6,000,000 transactions per year. Any merchant that has suffered a breach that resulted in an account data compromise. Any merchant that a card network provider determines “at its sole discretion” should meet the Level 1 merchant requirements to minimize risk to their respective system.	Required Annually		Required Quarterly Satisfied with TraceSecurity
Level 2 Any merchant – regardless of acceptance channel – processing 1,000,000 to 6,000,000 transactions per year.		Required Annually Satisfied with TraceSecurity	Required Quarterly Satisfied with TraceSecurity
Level 3 Any merchant processing 20,000 to 1,000,000 e-commerce transactions per year.		Required Annually Satisfied with TraceSecurity	Required Quarterly Satisfied with TraceSecurity
Level 4 Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants - regardless of acceptance channel - not in Levels 1, 2, or 3.		Required Annually Satisfied with TraceSecurity	Required Quarterly Satisfied with TraceSecurity
SERVICE PROVIDERS			
Level 1 All processors and all payment gateways.	Required Annually		Required Quarterly Satisfied with TraceSecurity
Level 2 Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 accounts/transactions annually.	Required Annually		Required Quarterly Satisfied with TraceSecurity
Level 3 Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 accounts/transactions annually.		Required Annually Satisfied with TraceSecurity	Required Quarterly Satisfied with TraceSecurity

About TraceSecurity

TraceSecurity is a leading provider of security compliance and risk management solutions. The company helps organizations of all sizes to achieve, maintain and demonstrate security compliance while significantly improving their security posture. Key to TraceSecurity’s success is the company’s comprehensive patent-pending methodology that helps clients address all of the critical components of a successful security compliance program: people, process and technology.

TraceSecurity delivers its solutions through an integrated software-as-a-service platform backed by expert professional services and comprehensive security awareness programs. The company’s flagship offering, TraceSecurity Compliance Manager, is the first comprehensive

solution to automate regulatory compliance audits, board-level reporting, policy management, vulnerability assessment, and employee education and testing. The company’s expert professional services include onsite risk assessments, security audits, and social engineering. The security awareness programs include an exhaustive set of standard offerings as well as custom-designed courses. With over 500 clients, TraceSecurity supports the risk management and security compliance efforts of organizations in financial services, healthcare, insurance, government and other regulated sectors.