Payment Card Industry Overview

Standard PCI Requirements

- **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.
- **Requirement 3**: Protect stored cardholder data.
- **Requirement 4**: Encrypt transmission of cardholder data across open, public networks.
- **Requirement 5**: Use and regularly update antivirus software.
- **Requirement 6**: Develop and maintain secure systems and applications.
- **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.
- **Requirement 10**: Track and monitor all access to network resources and cardholder data.
- **Requirement 11**: Regularly test security systems and processes.
- **Requirement 12**: Maintain a policy that addresses information security.

The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of comprehensive requirements for enhancing payment account data security—developed by the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. The goal of PCI is to increase protection of customer credit card information. The 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 full standard is available at: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml .

Customers should review this document independently, but we have summarized some of their compliance statements at the left. Cisco® Compliance Recording and Quality Management meets the PCI requirements that address the application layer. It is important to note, however, that most of the compliance requirements center on the network environment. Cisco has documented its network compliance in the document **Payment Card Industry Compliance on Cisco® Catalyst® Series Switches**; the documentation is available at: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/ps713/aag_c45_484784_v1.pdf.

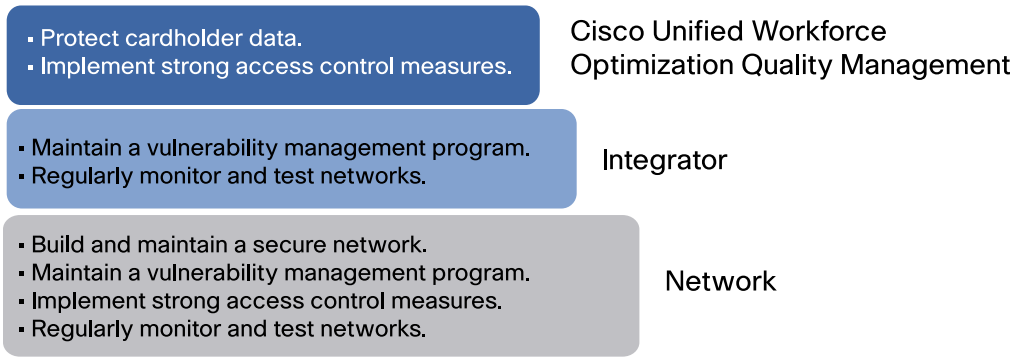
Following is summary of the PCI DSS requirements, followed by details about the way in which the Cisco Compliance Recording and Quality Management solution addresses these requirements at the application layer.

Requirements 1, 2, 6, 7, 8, and 10 are all functions of the customer network infrastructure environment and the features invoked during deployment by the network or system integrator. The Cisco documentation noted previously specifies the following features provided to address these requirements:

- VLAN segmentation protects customer data (requirement 1).
- Standard 802.1x authentication restricts access to customer data (requirements 7 and 8).
- Access to the switches is encrypted using Secure Shell Protocol (requirements 2 and 8)
- Access is restricted and logged by using built-in authentication techniques (requirements 2 and 8).
- Timed session terminations are implemented (requirements 2 and 8).
- Network usage is audited by tracking users through integrated, hardware-enabled Cisco NetFlow (requirement 10).

The customer or system integrator must address requirements 5, 6, 11, and 12. Requirements 3, 4, 7, 8, and 9 are functions of the application addressed within the Cisco Compliance Recording and Quality Management software itself.

Figure 1. PCI Compliance by Solution Component



Cisco provides an application programming interface (API) that enables users to stop and start recording during a transaction to prevent credit card and other personal data from being recorded through voice or screen. Using the recording API, contact centers can prevent Cisco Compliance Recording and Quality Management from capturing portions of audio containing card validation codes, personal identification numbers (PINs), or personal-area-network (PAN) numbers. The API enables contact centers to create recording pause functions, which can be controlled through integration with other transaction programs (that is, presented to the agent with Cisco Agent Desktop custom buttons) (requirement 3—specifically 3.2.2, 3.2.3, and 3.3—and requirement 9).

Cisco Compliance Recording and Quality Management offers the following benefits:

- Cisco Compliance Recording and Quality Management temporarily caches recorded content in a proprietary format on a protected directory with read and write permissions disabled for all users.
- These files are compressed and encrypted using the Advanced Encryption Standard (AES-128-CBC) before they are transported over the network and stored on the storage server. In cases where the transport includes any open, public networks, it is recommended that a VPN be used to provide additional security. This VPN prevents users from accessing stored files or files that may be intercepted while being transported over the network (requirements 3 and 4).
- Cisco Compliance Recording and Quality Management provides role-based access whereby certain users have privileges for access to certain recordings. This function provides the capability to limit users from accessing some recordings, such as restricting access to cardholder data based on their need to know. Users must be configured and licensed by an administrator before they can access the system meeting. The default is no access (requirement 7, specifically 7.1 and 7.2)
- Cisco Compliance Recording and Quality Management takes advantage of Microsoft Active Directory services for user authentication to enable the strong access control measures required by the PCI specification. Active Directory configuration options meet specific requirements for user ID assignment, first-time passwords, use termination, time-limited accounts, password strength, time limits, and lockouts. In addition, the Cisco Compliance Recording and Quality Management desktop application enforces configurable session timeout limits and requires reauthentication when a user exceeds the inactivity time limit. The application meets database access security requirements through configuration options provided by the Microsoft SQL 2005 database (requirements 8.1–8.5).

For further information, contact your certified Cisco Compliance Recording and Quality Management system integrator.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-570478-00 02/10