

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 anti-virus 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

PCI Overview

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 can be found 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 to the left.

Calabrio Compliance Recording and Quality Management meets the PCI requirements that address the application layer. Most, if not all, of the compliance requirements center on the network environment. In a Cisco environment, for example, many of the requirements would fall to the Cisco network and/or the integrator.

Here is summary of the PCI DSS requirements, followed by details about the way in which the Calabrio Compliance Recording and Quality Management solution addresses these requirements. Cisco has documented their compliance in the document **Payment Card Industry Compliance on Cisco Catalyst Series Switches**, which can be found at this link:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/ps713/aag_c45_484784_v1.pdf

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. Cisco's document specifies the following features that they provide to address these requirements:

- > VLAN segmentation (Requirement 1)
- > 802.1x authentication (Requirements 7 and 8)
- > Encrypt access to the switches using Secure Shell Protocol (Requirement 2 and 8)
- > Restrict and log access using built-in authentication techniques (Requirement 2 and 8)
- > Implement timed session terminations (Requirement 2 and 8)
- > Track users through integrated, hardware-enabled Cisco NetFlow to audit network usage (Requirement 10)

Requirement 5, 6, 11 and 12 must be addressed by the customer or system integrator.

Requirements 3, 4, 7, 8 and 9 are functions of the application addressed within the Calabrio Compliance Recording and Quality Management software itself.

PCI Compliance by Solution Component

- > Protect Cardholder Data
- > Implement Strong Access Control Measures

Calabrio
Quality Management

- > Maintain a Vulnerability Management Program
- > Regularly Monitor and Test Networks

Integrator

- > Build and Maintain a Secure Network
- > Maintain a Vulnerability Management Program
- > Implement Strong Access Control Measures
- > Regularly Monitor and Test Networks

Network

- > Calabrio provides an API that enables users to stop and start recording during a transaction to prevent credit card and other personal data from being recorded via voice and/or screen. Using the recording API, Contact centers can prevent Calabrio Compliance Recording and Quality Management from capturing portions of audio containing card validation codes, PINs or PAN numbers. The API enables contact centers to create recording pause functionality, which can be controlled through integration with other transaction programs (i.e. presented to the agent via Cisco Agent Desktop custom buttons.) (Requirement 3 - specifically 3.2.2; 3.2.3 and 3.3 - and Requirement 9)
- > Calabrio 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 Advanced Standard Encryption (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 prevents users from accessing stored files or files that may be intercepted while being transported over the network. (Requirements 3 and 4)

- > Calabrio 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 prior to being able to access the system meeting. The default is no access. (Requirement 7, Specifically 7.1, 7.2)
- > Calabrio Compliance Recording and Quality Management leverages Microsoft's 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, user termination, time limited accounts, password strength, time limits and lockouts. In addition, the Calabrio Compliance Recording and Quality Management desktop application enforces configurable session timeout limits and requires re-authentication once 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/Calabrio Compliance Recording and Quality Management system integration.

calabrio™

There's no end to better.

605 Highway 169 North • Minneapolis MN • 55441
763.592.4600 • www.calabrio.com

© Copyright 2008, Calabrio, Inc. All rights reserved.
Calabrio and the Calabrio logo are the registered trademark of Calabrio.
All other products are the property of their respective companies. SBRO-20080801