

Using Automated, Detailed Configuration and Change Reporting to Achieve and Maintain PCI Compliance—Part 3

An in-depth look at Payment Card Industry Data Security Standard Requirements 5, 6, 7, 8, 9

Alex Bakman
Chairman and Chief Technology Officer
Ecora Software

Introduction

In 2004, all major bankcards—Visa, MasterCard, Discover, and American Express—adopted a single, unified program as the standard for data security. The new standard, called the Payment Card Industry Data Security Standard or PCI, is intended to protect cardholder data—wherever it resides or is transmitted—and requires that merchants and service providers that store, process, or transmit cardholder data meet specific security requirements.

Ensuring compliance with the PCI standard is important to organizations for a number of reasons, particularly to protect brand reputation and to avoid fines and additional regulatory scrutiny.

Who Must Be In Compliance?

At the most fundamental level, any company that comes into contact with credit card information must be in compliance with the PCI Data Security Standard.

There are varying levels of compliance proof or validation, however, with specific requirements for merchants and specific requirements for service providers, as well as distinct compliance levels based on the number of transactions processed annually by the merchant or service provider.

For more introductory information about the Payment Card Industry Data Security Standard, download the Ecora whitepaper: **Using Automated, Detailed Configuration and Change Reporting to Achieve and Maintain Payment Card Industry Compliance**. For a detailed look at PCI requirements 1, 2, 3, and 4, download the Ecora whitepaper: **Using Automated, Detailed Configuration and Change Reporting to Achieve and Maintain Payment Card Industry Compliance: An in-depth look at Payment Card Industry Data Security Standard Requirements 1, 2, 3, 4**.

Meeting the PCI Data Security Standard Requirements

The Payment Card Industry Data Security Standard establishes twelve requirements that companies must follow to ensure the security of credit card data. These requirements span every aspect of an organization's operation—from business processes to the configuration of the IT infrastructure—and fall into six major control objectives:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Scope of Assessment for PCI Compliance

The PCI Data Security Standard requirements apply to all “system components” or any network component, server, or application that is included in or connected to the cardholder data environment. This means that even remote employees who have access to cardholder data must be in compliance with PCI.

A service provider or merchant may use a third-party provider to manage system components, but, because there may be an impact on the security of the cardholder data environment, the services of the third-party provider must be evaluated either in 1) the PCI audits of the third-party provider's clients or 2) the third-party provider's own PCI audit. There is really no distinction between your environment and an outsourced environment.

For merchants required to undergo an annual onsite review, the scope of compliance validation is focused on any system or system components related to transaction authorization and settlement where cardholder data is stored, processed, or transmitted. Service providers required to undergo an annual onsite review must perform compliance validation on all system components where cardholder data is stored, processed, or transmitted, unless otherwise specified.

During a PCI audit, auditors will typically select a sample of firewalls, routers, wireless access points, databases, applications, etc. that is large enough to validate findings representative of the entire environment. Importantly, the more standardized the environment—a single operating system, a single database vendor, etc.—and the more clearly configuration standards are defined, the smaller the sample required. Standardization provides many valuable benefits, among them is reducing the scope of an audit.

PCI Data Security Standard Requirements

Build and Maintain a Secure Network

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

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

Protect Cardholder Data

Requirement 3: Protect stored data.

Requirement 4: Encrypt transmission of cardholder data and sensitive information across 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 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.

While the twelve requirements of the PCI Data Security Standard may appear quite broad at first glance, each consists of numerous sub-requirements that make ensuring PCI compliance far more complex.

In this whitepaper, we will discuss requirements five through nine of the PCI Data Security Standard and their sub-requirements in detail—as outlined in version 1.1 of the standard, which was released and updated in September 2006—to demonstrate the level of scrutiny and validation an organization can expect during an internal audit.

Requirement 5: Use and regularly update anti-virus software or programs.

Anti-virus software provides organizations with the first line of defense against malicious attacks and other vulnerabilities and is a “must have.” Organizations need to ensure—and demonstrate—that the latest signature file is distributed in a timely manner to all systems commonly affected by viruses.

Requirement 6: Develop and maintain secure systems and applications.

Under this requirement, an organization ensures that the entire infrastructure involved in credit card processing is updated as soon as security patches are provided. PCI auditors look for specific evidence that this practice is taking place, so it is critical that the process be clearly documented. All systems must have the most recently released, appropriate software patches installed to protect against exploitation by employees, external hackers, and viruses.

System Name	Operating System	Missing Patches	Percentage Installed
ECORAQA.ALBANY	Operating System: Windows 2000 Advanced Server	Missing Internet Information Services 5.0 Patches	100% - 0 out of 2 patches installed
		Missing MDAC 2.5 Patches	100% - 0 out of 1 patches installed
		Missing Windows 2000 Advanced Server Patches	85% - 5 out of 34 patches installed
		Missing Windows Media Player 6.4 For Windows 2000 Patches	80% - 1 out of 5 patches installed
ECORAQA.BOSTON	Operating System: Windows 2000 Advanced Server	Missing MDAC 2.6 Patches	100% - 0 out of 1 patches installed
		Missing SQL Server 2000 Patches	100% - 0 out of 6 patches installed
		Missing Windows 2000 Advanced Server Patches	66% - 2 out of 6 patches installed
		Missing Windows Media Player 6.4 For Windows 2000 Patches	100% - 0 out of 5 patches installed
ECORAQA.DENVER	Operating System: Windows XP Professional	Missing Internet Explorer 6 Patches	100% - 0 out of 15 patches installed
		Missing MDAC 2.7 Patches	100% - 0 out of 3 patches installed
		Missing Windows Media Player for Windows XP Patches	100% - 0 out of 3 patches installed
		Missing Windows XP Professional Patches	86% - 5 out of 38 patches installed
ECORAQA.NEWYORK	Operating System: Windows 2000 Advanced Server	Missing MDAC 2.5 Patches	100% - 0 out of 1 patches installed
		Missing SQL Server 7.0 Patches	100% - 0 out of 4 patches installed
		Missing Windows 2000 Advanced Server Patches	66% - 2 out of 6 patches installed
		Missing Windows Media Player 6.4 For Windows 2000 Patches	100% - 0 out of 5 patches installed

Ecora's Missing Patches Summary Report fulfills PCI DSS 6.1.a, “For a sample of system components, critical servers, and wireless access points and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.”

Computers Without Antivirus Software Installed

Prepared For: Mr. John Customer <Customer@ecora.com>
 Prepared On: 10/24/2006 8:07:42 AM
 Prepared By: Ecora Auditor Professional 4.0 - Windows Module
 Prepared Using: FFR Definition 'Computers Without Antivirus Software Installed'
 Prepared Time Criteria: Last 20 week(s)
 Copyright © 2006 Your Organization
 All rights reserved.

PCI section 5.2 This report includes the computer name of systems that do not have an Antivirus application installed. If all systems have an Antivirus application installed, then it will state "No relevant data found".

Domain	Computer
COMPLIANCE.ORG/ECORA-DC.COMPLIANCE.ORG	
COMPLIANCE/AUDITORDENO	
COMPLIANCE/ECORA-DC	
COMPLIANCE/SHARDPOINT	
TEST.LOCAL/CLUSTER1	

Ecora's Computers Without Antivirus Software Installed Report fulfills PCI DSS 5.1, “For a sample of system components, critical servers, and wireless access points, verify that anti-virus software is installed.”

Requirement 5.1

Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers).

Sub-requirement 5.1.1: Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.

In this instance, the auditor will work with a sample of an organization's desktop systems, etc. to validate that anti-virus software is installed and functioning.

Requirement 5.2

Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

Auditors will also look to be sure that signature files are up to date and there is a process in place to update and distribute the latest signature files. Ultimately, they use audit logs to ensure anti-virus software is configured and functioning properly.

Requirement 6.1

Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

Most organizations understand how important it is to ensure that security patches are up to date, but some may be surprised by PCI's requirement that patches must be applied within 30 days of release. If this requirement matches with an organization's existing patch-application cycle, then that organization is in compliance; if it does not, then the organization will need to modify its processes to ensure compliance.

Requirement 6.2

Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.

To satisfy this requirement, organizations should demonstrate a clear process for learning about new security vulnerabilities. Some organizations satisfy this requirement by subscribing to a free alert service, such as the one available from Carnegie Mellon University. If an organization is using an automated patch management system, it can satisfy the requirement by demonstrating how it processes new patches when they are released.

Requirement 6.3

Develop software applications based on industry best practices and incorporate information security throughout the software development lifecycle.

Sub-requirement 6.3.1: Testing of all security patches and system and software configuration changes before deployment

Sub-requirement 6.3.2: Separate development, test, and production environments

Sub-requirement 6.3.3: Separation of duties between development, test, and production environments

Sub-requirement 6.3.4: Production data (live PANs) are not used for testing or development

Sub-requirement 6.3.5: Removal of test data and accounts before production systems become active

Sub-requirement 6.3.6: Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers

Sub-requirement 6.3.7: Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability

In this requirement, PCI outlines objectives for in-house software development, with the ultimate goal being the clear, documented separation of roles and responsibilities of the development, test, and production environments; of test data; and of accounts. Adhering to these requirements may be routine for many organizations, however, it is important the processes are documented to demonstrate compliance. For example, an organization should be able to show that newly-developed application updates go through an assessment process where patches are applied and then the application is retested.

Organizations should also be able to validate that no one person can take an application from development, to test, to production by clearly identifying hand-offs, and that best practices are utilized to ensure security when working with test data and account information.

Requirement 6.4

Follow change control procedures for all system and software configuration changes. The procedures must include the following:

Sub-requirement 6.4.1: Documentation of impact

Sub-requirement 6.4.2: Management sign-off by appropriate parties

Sub-requirement 6.4.3: Testing of operational functionality

Sub-requirement 6.4.4: Back-out procedures

PCI auditors are concerned with how frequently an organization upgrades applications, the quality processes involved, whether there is a traceability index, and whether changes to each application can be specifically identified. The requirement addresses two types of changes in particular: source code changes and infrastructure changes. As is the case with most security requirements, this specifies an organization have an iron-clad change-management process in place to ensure that changes are recorded, approved (with appropriate sign-off), and validated within the environment.

Not all changes are appropriate, so an organization should also have a back-out procedure in place for each change, which is clearly documented as part of the change control system. The requirement also mandates adequate testing before a patch is applied to production

systems and that a solid change control process is in place for all systems and self-reconfigurations.

Requirement 6.5

Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:

Sub-requirement 6.5.1: Unvalidated input

Sub-requirement 6.5.2: Broken access control (for example, malicious use of user IDs)

Sub-requirement 6.5.3: Broken authentication and session management (use of account credentials and session cookies)

Sub-requirement 6.5.4: Cross-site scripting (XSS) attacks

Sub-requirement 6.5.5: Buffer overflows

Sub-requirement 6.5.6: Injection flaws (for example, structured query language (SQL) injection)

Sub-requirement 6.5.7: Improper error handling

Sub-requirement 6.5.8: Insecure storage

Sub-requirement 6.5.9: Denial of service

Sub-requirement 6.5.10: Insecure configuration management

Organizations should follow guidelines for web application development, such as those from the Open Web Application Security Project (www.oasp.org), which describes how to develop and maintain best practices for designing web applications. The PCI requirements cited above follow these guidelines for developing secure web applications.

One of the first steps towards meeting these requirements is to test all customer-facing applications to identify any malicious activity or threats. Organizations should identify invalid access controls and invalid IDs, as well as common hacker techniques such as broken authentication and session management, cross-site scripting attacks, and Denial of Service attacks. Auditors will evaluate how an infrastructure responds to threats and errors, as well as how secure configurations are in the database management environment.

Requirement 6.6

Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:

- Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security
- Installing an application-layer firewall in front of web-facing applications.

Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.

If application development has not been reviewed by a qualified third party specializing in application security, it should be implemented as a standard. Large organizations spend a great deal of time reviewing code. Microsoft, for example, has stopped software development to go through an exercise where source code is reviewed by experts familiar with security. In addition to helping demonstrate compliance, this process can provide "peace of mind" to those responsible for credit

card processing applications, by enabling them to go through an independent review, and then document the findings, any required remediation, and the results.

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

This requirement ensures critical data can only be accessed by authorized personnel. To meet this requirement, organizations must document each specific organizational function and demonstrate that each staff member performs that function only. They must also show who has access to which systems and data. A delineation of functions helps ensure that no one in the organization has access to the entire procedure for processing credit card data.

Requirement 7.1

Limit access to computing resources and cardholder information to only those individuals whose job requires such access.

Requirement 7.2

Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.

In the case of requirements 7.1 and 7.2, auditors will look for evidence that an organization has procedures in place to assign access rights to users; that systems are set up to deny access unless it is specifically required, and that access to information such as cardholder data is granted only under very specific conditions and only to those who need to have access. These procedures must be in place for all system components that transmit or store cardholder data.

Sites with Anonymous Access

Prepared For: Mr. John Customer <Customer@ecora.com>
 Prepared On: 10/26/2006 3:30:25 PM
 Prepared By: Ecora Auditor Professional 4.0 - MS ITD Module
 Prepared Using: FFR Definition 'Sites with Anonymous Access'
 Prepared Time Criteria: Last 20 week(s)
 Copyright © 2006 Your Organization
 All rights reserved.

Requirement 7 - Section 7.1 - Description for Sites with Anonymous Access

Table 1. Sites with Anonymous Access		
Name	Anonymous Username	Anonymous Access
audstordemo	IUSR_AUDITOR	Enabled
ecora-dc	IUSR_ECORA-DC	Enabled

Ecora's Sites with Anonymous Access Report fulfills PCI DSS 7.1, "Obtain and examine written policy for data control, and verify that the policy incorporates the following: Access rights to privileged user IDs are restricted to least privileges necessary to perform job responsibilities, assignment of privileges is based on individual personnel's job classification and function, and implementation of an automated access control system."

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

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Organizations should have a written policy in place, signed by each employee, that states that all IDs and credentials are to be used solely by the individual to whom they are assigned. PCI standards intend an organization to have visibility down to the individual level so that an audit trail can be compiled to show who did what to which system and when.

Organizations should also ensure they have a policy for password aging and that password aging can be verified and validated. If, for example, a policy mandates that passwords should be changed every thirty days, an organization should be able to prove that is indeed the case.

PCI section 8.1 and 8.5 This report contains four tables: (1) Domain Password Policy Settings, (2) Local Computer Password Policy Settings, (3) Domain Account Lockout Policy, and (4) Local Computer Account Lockout Policy. Review these policies and set according to corporate guidelines. Adhere to Microsoft, SANS or other security best practice guidelines if in doubt.

Table 1. Domain Password Policy Settings				
Domain Name	Min Password Length	Max Password Age	Min Password Age (Days)	Password History (Uniqueness)
COMPLIANCE.ORG	8	>=2 days	2	24

Table 2. Local Password Policy Settings				
Domain Computer	Min Password Length	Max Password Age	Min Password Age (Days)	Password History (Uniqueness)
COMPLIANCE.ORG/ECORA-DC.COMPLIANCE.ORG	8	42days	2	24
COMPLIANCE/AUDITORDEMO	1	42days	2	24
COMPLIANCE/ECORA-DC	8	42days	2	24
COMPLIANCE/SHAREPOINT	7	42days	2	24
TEST.LOCAL/CLUSTER1				

Table 3. Domain Account Lockout Policy					
Domain Name	Account Lockout Enabled	Account Lockout Threshold	Account Lockout Duration (Minutes)	Account Lockout Window (Minutes)	Force Logoff
COMPLIANCE.ORG	Yes	50	30	30	No

Table 4. Local Account Lockout Policy					
Domain Computer	Account Lockout Enabled	Account Lockout Threshold	Account Lockout Window (Minutes)	Account Lockout Duration (Minutes)	Force Logoff
COMPLIANCE.ORG/ECORA-DC.COMPLIANCE.ORG	Yes	50	30	30	Forced off immediately
COMPLIANCE/AUDITORDEMO	Yes	50	30	30	Forced off immediately
COMPLIANCE/ECORA-DC	Yes	50	30	30	Forced off immediately
COMPLIANCE/SHAREPOINT	Yes	50	30	30	Forced off immediately
TEST.LOCAL/CLUSTER1	No				

Ecora's Password and Account Lockout Report fulfills PCI DSS 8.5.15, "For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that system/session idle time out features have been set to 15 minutes or less."

Requirement 8.1

Identify all users with a unique user name before allowing them to access system components or cardholder data. Auditors will review whether or not each user has a unique ID.

Requirement 8.2

In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

- Password
- Token devices (e.g., SecureID, certificates, or public key)
- Biometrics

Organizations should add an additional layer of security to protect cardholder data.

Requirement 8.3

Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

To gain access to an organization's systems remotely, users must be authorized using two-factor authentication. A number of technologies can provide this level of authentication, with RADIUS being the most common.

Requirement 8.4

Encrypt all passwords during transmission and storage on all system components. Passwords should never be passed in clear text; they must always be encrypted.

Requirement 8.5

Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:

- Sub-requirement 8.5.1: Control addition, deletion, and modification of user IDs, credentials, and other identifier objects

Sub-requirement 8.5.2: Verify user identity before performing password resets

Sub-requirement 8.5.3: Set firsttime passwords to a unique value for each user and change immediately after the first use

Sub-requirement 8.5.4: Immediately revoke access for any terminated users

Sub-requirement 8.5.5: Remove inactive user accounts at least every 90 days

Sub-requirement 8.5.6: Enable accounts used by vendors for remote maintenance only during the time period needed

Sub-requirement 8.5.7: Communicate password procedures and policies to all users who have access to cardholder data

Sub-requirement 8.5.8: Do not use group, shared, or generic accounts and passwords

Sub-requirement 8.5.9: Change user passwords at least every 90 days

Sub-requirement 8.5.10: Require a minimum password length of at least seven characters

Sub-requirement 8.5.11: Use passwords containing both numeric and alphabetic characters

Sub-requirement 8.5.12: Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used

Sub-requirement 8.5.13: Limit repeated access attempts by locking out the user ID after not more than six attempts

Sub-requirement 8.5.14: Set the lockout duration to thirty minutes or until administrator enables the user ID

Sub-requirement 8.5.15: If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

Sub-requirement 8.5.16: Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users

Organizations should ensure that they have a clearly documented process for the creation of IDs, suspension of IDs, and ID management, including password resets. Auditors will focus on how the process works, and that all users understand password procedures; auditors are likely to interview select users to gauge their understanding of the procedure.

Organizations should always revoke access for terminated users immediately and remove inactive user accounts. Auditors will monitor this particular requirement closely, particularly for those users who had broad access to systems. It is important that this is closely coordinated with the human resources department. In addition, organizations should be sure that accounts set up for third parties are valid only when they are needed.

For reasons of traceability, there should be no shared, group, or generic accounts and passwords, so auditors will be looking to confirm that an organization has only unique IDs.

Organizations should change user passwords at least every 90 days, and ensure that they have a policy in place for password aging that can be verified and validated. If, for example, an organization has a policy that passwords should be changed every thirty days, they should be able to prove that is indeed the case. In addition, all passwords should meet specific criteria: be at least seven characters long and be distinct from at least the most recent four passwords used, for example. These criteria can be enforced by setting up a password policy in most systems.

Organizations should lock out a user after six failed access attempts, although many organizations have an even stricter policy that locks out users after three unsuccessful log-in attempts. Lockout duration should be set to 30 minutes or until an administrator unlocks the ID. A good credential management system will enable an organization to enforce this requirement automatically. In addition, if a session has been idle for more than 15 minutes, an organization should require the user to re-enter the password to re-activate the terminal.

Organizations should review configuration settings for a sample of databases to ensure that data access is authenticated for individual users and applications. Only authenticated users, applications, administrators, etc. should be granted access to any database containing cardholder data.

Requirement 9: Restrict physical access to cardholder data.

Without physical security, real infrastructure security cannot exist. Physical access to data or systems where cardholder data is stored should be closely monitored; any threat where unauthorized personnel may access devices or data, or remove systems or hardcopies should be eliminated.

Requirement 9.1

Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.

Sub-requirement 9.1.1: Use cameras to monitor sensitive areas. Audit collected data and correlate with other log entries. Store for at least three months, unless otherwise restricted by law

Sub-requirement 9.1.2: Restrict physical access to publicly accessible network jacks

Sub-requirement 9.1.3: Restrict physical access to wireless access points, gateways, and handheld devices

To meet this requirement, organizations need to monitor access in sensitive areas and implement procedures to track anyone entering or exiting the environment, including the use of security cameras and physical entry controls, such as a badge reader. The logs collected identifying who has entered the data center, including date and time, should be retained for at least three months.

In addition, physical access to publicly accessible network jacks, such as those in conference rooms, as well as to wireless access points, gateways, and handheld devices should be closely controlled, and should be enabled only when needed by authorized employees. Auditors will verify that these procedures are in place by interviewing network administrators and by observation. Visitors should be escorted at all times in any areas with network or wireless access.

Requirement 9.2

Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on the entity’s site. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.

Most organizations with mature data centers meet this requirement already using badges, a sign-in and sign-out process for guests, etc.

Requirement 9.3

Make sure all visitors are handled as follows:

Sub-requirement 9.3.1: Authorized before entering areas where cardholder data is processed or maintained

Sub-requirement 9.3.2: Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees

Sub-requirement 9.3.3: Asked to surrender the physical token before leaving the facility or at the date of expiration.

An organization should have visitor controls in place, including an authorization process and clear identification, such as visitor ID badges. All visitor badges should identify visitors as non-employees and clearly indicate expiration time. Auditors will verify through observation that the policy is followed in actual practice in the same manner it is documented.

Requirement 9.4

Use a visitor log to maintain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.

Auditors will review an organization’s visitor log to ensure that all requirements are met, that the visitor IDs used match the time of departure of the visitor and that the access was suspended, for example. It is also important to ensure that any physical audit trail is stored in a safe location, in an encrypted format, and with good physical security.

Requirement 9.5

Store media back-ups in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility.

It is likely that most organizations do this already to ensure preparedness in the event of disaster recovery. If not, it should become standard practice.

Requirement 9.6

Physically secure all paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data.

In addition to making sure that any physical copies of cardholder data is stored in a secure location, auditors will inspect how media is handled throughout an organization to ensure security.

Requirement 9.7

Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data including the following:

Sub-requirement 9.7.1: Classify the media so it can be identified as confidential

Sub-requirement 9.7.2: Send the media by secured courier or other delivery method that can be accurately tracked.

An organization should have documented procedures for handling all cardholder data and a clear tracking system so media can be located at any point in time. Any media that contains cardholder data should be marked as confidential, and should tightly controlled—even when in transit.

Requirement 9.8

Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).

An organization should ensure that a sign-out process, including an authorized signature, is in place for any media that is moved; this provides a clear audit trail.

Requirement 9.9

Maintain strict control over the storage and accessibility of media that contains cardholder data.

Sub-requirement 9.9.1: Properly inventory all media and make sure it is securely stored.

Solid management practices can ensure strict control of data in most organizations. If these practices are in place and if an organization is in compliance with the other requirements outlined above, then this requirement will be met by default.

Requirement 9.10

Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:

Sub-requirement 9.10.1: Cross-cut shred, incinerate, or pulp hardcopy materials

Sub-requirement 9.10.2: Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.

Organizations should implement a clear, written policy that outlines the procedures for destroying any media containing cardholder data. Any hardcopy materials or any other physical media should be destroyed according to specific instructions, and the method of physical destruction of media required should ensure the information contained on the media cannot be reconstructed.

How Ecora Software Can Help Organizations Ensure PCI Compliance

Ecora Software can help organizations demonstrate compliance to pass the 10 IT-related PCI audit sections efficiently, painlessly, and successfully.

Automation allows organizations to meet IT audit and compliance requirements without the investment in time and resources, but this approach can only work if an organization has the ability to identify and report on the entire infrastructure. Ecora covers all critical infrastructure components, from operating systems, network devices and firewalls, to mail servers, application enablers, and directory services, automatically collecting hundreds of thousands of critical configuration settings needed to recover, secure, report on, and track infrastructure changes.

Ecora discovers an organization's critical systems and collects configuration data—including security-related data such as credentials, permissions, access controls, and more. Data is stored in a relational database so that organizations can generate reports as needed to assess controls, identify configuration problems, do baseline comparisons, pinpoint deviations, generate change reports down to specific configuration settings, and compile comprehensive documentation reports for disaster recovery or explanatory reports for auditors.

In addition, Ecora's executive dashboard enables organizations to measure compiled data against a best-practice security policy to see the status of systems at a glance. For example, the dashboard can clearly show which systems are compliant with the policy and, if noncompliant systems are identified, allow users to drill down to see what rules are being violated.

In the case of the PCI requirements and sub-requirements outlined in this whitepaper, Ecora Software can help organizations collect and verify a range of information. To demonstrate compliance with PCI requirements for up-to-date anti-virus software, for example, Ecora can generate a report that shows which systems have, or do not have, anti-virus software deployed. Similarly, in the case of vendor-supplied security patches, we can provide reports that show where patches are missing, and then automate patch deployment.

Ecora can also help organizations meet change management requirements for all system components. Ecora reports provide valuable information about access control attributes and status over a period of time; these reports enable an auditor to easily assess how valid an organization's control systems are.

To ensure ID control, Ecora reports can show which users have access to what components and which users are in what groups. We can also interrogate systems to identify disabled accounts and find anomalies. There are also automated reports that show password policy, minimum password length, password age, password history, and account lockout policy.

To be successful, an organization must demonstrate they have control of change in their environment. Organizations using industry best practices, including the detailed reporting Ecora provides for regulatory compliance audits and enabling IT Best Practices, will not only ensure a successful PCI audit, but also reap far-reaching benefits for other parts of the environment. In fact, the ability to control change will not only help ensure ongoing compliance, but will also improve underlying problem management and change management processes.

Find Out More

To learn more about how Ecora can help you achieve and maintain PCI compliance, call [877.923.2672](tel:877.923.2672) or [+1 603.436.1616](tel:+1603.436.1616), email sales@ecora.com, or visit us on the web at www.ecora.com.

About Ecora

Ecora Software is the market-proven leader in transforming enterprise-wide data into easy-to-understand reports for regulatory compliance and enabling IT best practices. The Company's Auditor Professional provides the only patented architecture proven to automate the collection and reporting of configuration information from the entire infrastructure, without agents. Ecora Software takes the cost and complexity out of compliance audits and adopting IT best practices for thousands of customers worldwide, including many of the Fortune 100. For more information, please visit the Company's Web site at www.ecora.com, or phone [603-334-1616](tel:603-334-1616).