ecora

WHITEPAPER

Using Automated, Detailed Configuration and Change Reporting to Achieve and Maintain PCI Compliance—Part 4

An in-depth look at Payment Card Industry Data Security Standard Requirements 10, 11, 12

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. In fact, the October 1, 2006 issue of the Wall Street Journal highlighted new efforts at Visa to step up PCI compliance enforcement and discussed heavy fines that have been levied on some of the nation's largest retailers.

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*. For a detailed look at PCI requirements 5, 6, 7, 8, and 9, 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 5, 6, 7, 8, 9*.

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 on-site review, the scope of compliance validation is focused on any system or system components related to authorization and settlement where cardholder data is stored, processed, or transmitted. Service providers required to undergo an annual on-site 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 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 ten through twelve 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 on-site audit.

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

To successfully demonstrate PCI compliance, an organization must be able to monitor system access, whether to network devices, databases, operating systems, or any other component that must meet PCI requirements. This requirement focuses on monitoring the actual access to systems, using audit trails, logs, etc.

Requirement 10.1

Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user. All access, even by administrative staff, must be logged to ensure easy auditing. Using logging tools to track user access and activities on the systems that store cardholder data, and then having that data available for analysis, is especially important.

Requirement 10.2

Implement automated audit trails for all system components to reconstruct the following events:

Sub-requirement 10.2.1: All individual user accesses to cardholder data

Sub-requirement 10.2.2: All actions taken by any individual with root or administrative privileges

Sub-requirement 10.2.3: Access to all audit trails

Sub-requirement 10.2.4: Invalid logical access attempts

Sub-requirement 10.2.5: Use of identification and authentication mechanisms

Sub-requirement 10.2.6: Initialization of the audit logs

Sub-requirement 10.2.7: Creation and deletion of system-level objects

Organizations must turn on "logging" in all systems that store cardholder data to audit individual access to data and audit trails, invalid access attempts, and the creation and deletion of objects within the system. Organizations should also deploy identification and authentication mechanisms to track and record security concerns.

Requirement 10.3

Record at least the following audit trail entries for all system components for each event:

Sub-requirement 10.3.1: User identification

Sub-requirement 10.3.2: Type of event

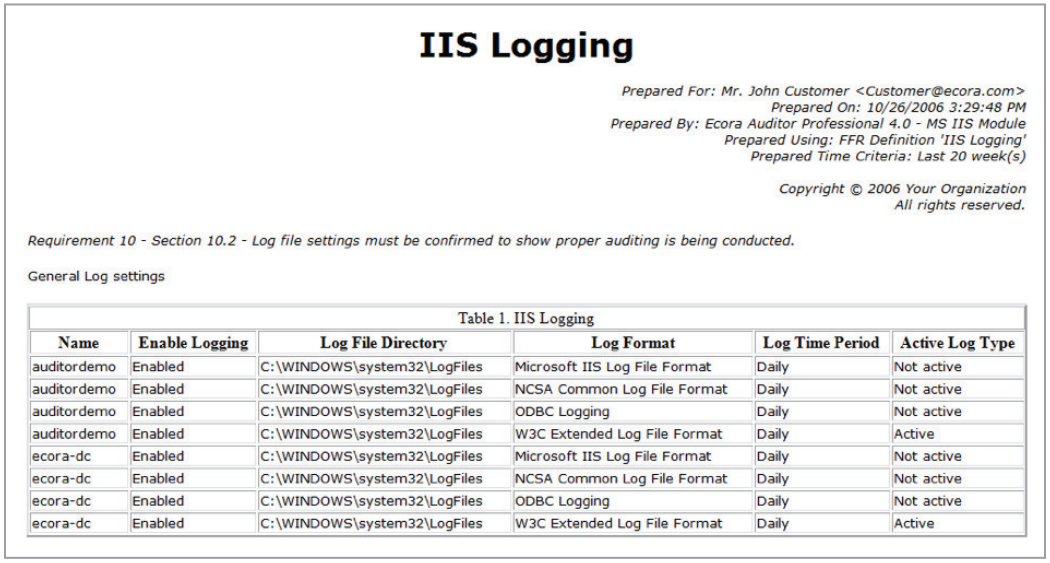
Sub-requirement 10.3.3: Date and time

Sub-requirement 10.3.4: Success or failure indication

Sub-requirement 10.3.5: Origination of event

Sub-requirement 10.3.6: Identity or name of affected data, system component, or resource.

This requirement specifically defines the format and the type of data organizations should collect in their audit trails.



IIS Logging

Prepared For: Mr. John Customer <Customer@ecora.com>
Prepared On: 10/26/2006 3:29:48 PM
Prepared By: Ecora Auditor Professional 4.0 - MS IIS Module
Prepared Using: FFR Definition 'IIS Logging'
Prepared Time Criteria: Last 20 week(s)

Copyright © 2006 Your Organization
All rights reserved.

Requirement 10 - Section 10.2 - Log file settings must be confirmed to show proper auditing is being conducted.

General Log settings

Table 1. IIS Logging

Name	Enable Logging	Log File Directory	Log Format	Log Time Period	Active Log Type
auditordemo	Enabled	C:\WINDOWS\system32\LogFiles	Microsoft IIS Log File Format	Daily	Not active
auditordemo	Enabled	C:\WINDOWS\system32\LogFiles	NCSA Common Log File Format	Daily	Not active
auditordemo	Enabled	C:\WINDOWS\system32\LogFiles	ODBC Logging	Daily	Not active
auditordemo	Enabled	C:\WINDOWS\system32\LogFiles	W3C Extended Log File Format	Daily	Active
ecora-dc	Enabled	C:\WINDOWS\system32\LogFiles	Microsoft IIS Log File Format	Daily	Not active
ecora-dc	Enabled	C:\WINDOWS\system32\LogFiles	NCSA Common Log File Format	Daily	Not active
ecora-dc	Enabled	C:\WINDOWS\system32\LogFiles	ODBC Logging	Daily	Not active
ecora-dc	Enabled	C:\WINDOWS\system32\LogFiles	W3C Extended Log File Format	Daily	Active

Ecora's IIS Logging Report helps fulfill PCI DSS 10.2.1, "Verify through audit logs that all individual access to cardholder data is logged into system activity logs."

Requirement 10.4
Synchronize all critical system clocks and times. The synchronization of system clocks is important primarily for security reasons. One of the techniques hackers commonly employed in their attempt to penetrate systems is to change system clocks to "fool" the system into thinking it is in "maintenance" mode. Organizations should use standard clock synchronization technology, as well as ensuring servers are not accessible externally or vulnerable to compromise.

Requirement 10.5
Secure audit trails so they cannot be altered.

Sub-requirement 10.5.1: Limit viewing of audit trails to those with a job-related need

Sub-requirement 10.5.2: Protect audit trail files from unauthorized modifications

Sub-requirement 10.5.3: Promptly back-up audit trail files to a centralized log server or media that is difficult to alter

Sub-requirement 10.5.4: Copy logs for wireless networks onto a log server on the internal LAN

Sub-requirement 10.5.5: Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)

Audit trails are reliable only if organizations can be confident that they have not been altered. To secure audit trail data, they should be protected from unauthorized access and modifications, and only those with a job-related need should be allowed to view them. Systems should be backed up and stored securely, and file integrity monitoring and change detection software should be deployed to ensure data cannot be altered without generating alerts.

Requirement 10.6
Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). The process of reviewing logs for all system components can be an incredibly time-consuming task if done manually, which is why organizations should consider meeting this requirement using log consolidation software to filter out and identify specific events.

Requirement 10.7
Retain audit trail history for at least one year, with a minimum of three months online availability. When an organization backs up audit trails and logs, the data should be archived securely, with the last three months worth of data easily accessible online. It is likely that a PCI auditor will ask to review an organization's audit trail history and will want information about how audit logs are retrieved and reviewed.

Requirement 11
Regularly test security systems and processes. With evolving threats and vulnerabilities, it is essential that organizations test all systems, processes, and software used with cardholder data to ensure that security is maintained.

Requirement 11.1
Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use. To ensure PCI compliance, systems within the cardholder environment should be tested at least once a year. If an organization uses wireless access points, security systems should be tested at least quarterly.

Requirement 11.2
Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). Many organizations already perform quarterly vulnerability scans. To ensure compliance with this requirement, it is especially important that scans are completed after any significant change in the environment, such as new system installations.

Requirement 11.3
Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:

Sub-requirement 11.3.1: Network-layer penetration tests

Sub-requirement 11.3.2: Application-layer penetration tests

To help ensure the validity of annual network- and application-layer penetration tests, it is valuable for an organization to involve an external organization with recognized testing experience. A test conducted by an experienced third party is likely to have more credibility with a PCI auditor.

Requirement 11.4
Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date. To ensure PCI compliance, organizations must have IDS or IPS in place. Auditors will check to confirm that such systems are installed and properly functioning, and will also ask for information about who has access to the systems, how often output is examined, etc.

Requirement 11.5
Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly. All critical system files should be monitored regularly to ensure that any changes are authorized. In addition to those that contain cardholder data, critical files include any file or component, which, if compromised, could make cardholder data vulnerable.

Requirement 12: Maintain a policy that addresses information security for employees and contractors. A strong, company-wide security policy is critical for PCI compliance. Ensuring that cardholder data is protected is an important responsibility for all employees, and all company personnel should understand their roles and responsibilities for security within the organization. Contractors should be expected to meet the same security requirements.

Requirement 12.1
Establish, publish, maintain, and disseminate a security policy that accomplishes the following:

Sub-requirement 12.1.1: Addresses all requirements in this specification

Sub-requirement 12.1.2: Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment

Sub-requirement 12.1.3: Includes a review at least once a year and updates when the environment changes

If an organization does not have a written security policy, it is definitely time to start putting one together. PCI provides a very comprehensive description of what a security policy should entail, and could serve as a helpful template for any organization without a security policy in place. In addition, the security policy should be reassessed and updated annually or when the environment changes—the policy cannot be static.

Requirement 12.2
Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures). Daily operational security procedures should clearly identify the tasks that an organization will perform on a daily basis to ensure compliance with the security policy.

Requirement 12.3
Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:

Sub-requirement 12.3.1: Explicit management approval

Sub-requirement 12.3.2: Authentication for use of the technology

Sub-requirement 12.3.3: List of all such devices and personnel with access

Sub-requirement 12.3.4: Labeling of devices with owner, contact information, and purpose

Sub-requirement 12.3.5: Acceptable uses of the technologies

Sub-requirement 12.3.6: Acceptable network locations for the technologies

Sub-requirement 12.3.7: List of company-approved products

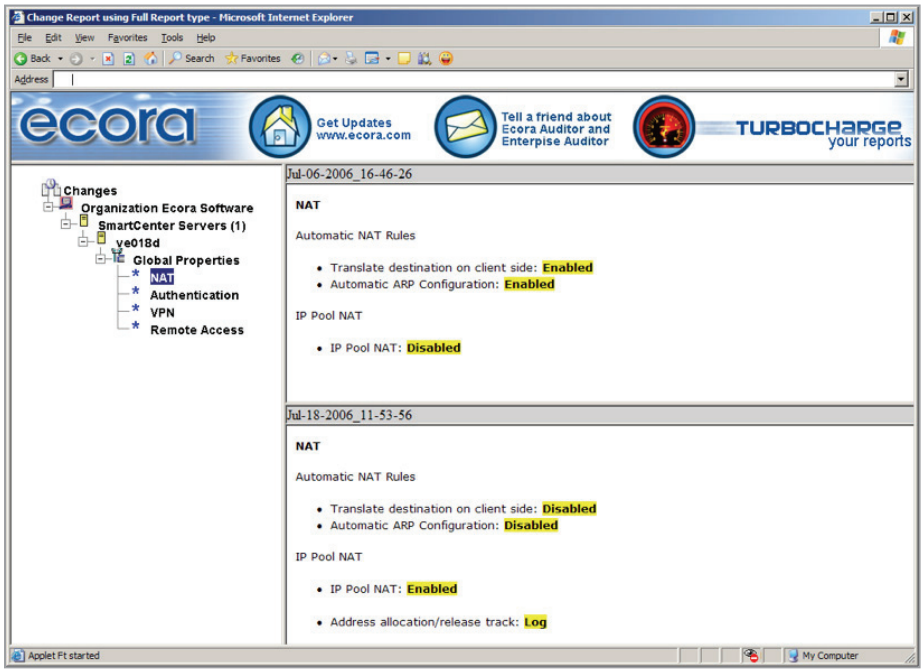
Sub-requirement 12.3.8: Automatic disconnect of modem sessions after a specific period of inactivity

Sub-requirement 12.3.9: Activation of modems for vendors only when needed by vendors, with immediate deactivation after use

Sub-requirement 12.3.10: When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access

Developing a solid usage process is important in any information security policy. This requirement outlines the specific elements that must be included in a usage process. The process should have management approval and user sign-off.

Requirement 12.4
Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors. Each employee's roles and responsibilities with regard to an organization's security policy should be incorporated into the job description. A contractor's responsibilities should be clearly outlined in the contract.



Ecora change reports help fulfill PCI DSS 11.2a, "Verify that periodic security testing of devices within the card holder environment occurs."

Requirement 12.5
Assign to an individual or team the following information security management responsibilities:

Sub-requirement 12.5.1: Establish, document, and distribute security policies and procedures

Sub-requirement 12.5.2: Monitor and analyze security alerts and information, and distribute to appropriate personnel

Sub-requirement 12.5.3: Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations

Sub-requirement 12.5.4: Administer user accounts, including additions, deletions, and modifications

Sub-requirement 12.5.5: Monitor and control all access to data

Organizations should outline and assign security management responsibilities. To ensure compliance, it is important to produce specific, clear documentation of roles, and to ensure that roles and responsibilities are understood by employees and contractors. Security policies should be documented and distributed, and incident response and escalation procedures should be clearly outlined. All access to data should be monitored and controlled, and access to user accounts should be clearly administered.

Requirement 12.6
Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.

Sub-requirement 12.6.1: Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)

Sub-requirement 12.6.2: Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures

An organization can have the world's best-sounding security policy, but if employees aren't educated about the policy and its requirements, it will be of little value. Security education efforts should be part of new-hire orientation and annual employee training, and employees should acknowledge in writing that they have read and understood the organization's security policy.

Requirement 12.7
Screen potential employees to minimize the risk of attacks from internal sources. To ensure compliance with PCI, there are important requirements that must be a part of all employee recruitment and hiring efforts. These should include personal references, a criminal background check, and a credit history. Employing these as hiring standards will help demonstrate to auditors that an organization is hiring employees in good standing.

Requirement 12.8
If cardholder data is shared with service providers, then contractually the following is required:

Sub-requirement 12.8.1: Service providers must adhere to the PCI DSS requirements

Sub-requirement 12.8.2: Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses

Organizations should validate that the service providers with whom they work are following the same policies as the organization, and that they are PCI compliant.

Requirement 12.9
Implement an incident response plan. Be prepared to respond immediately to a system breach.

Sub-requirement 12.9.1: Create the incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the Acquirers and credit card associations)

Sub-requirement 12.9.2: Test the plan at least annually

Sub-requirement 12.9.3: Designate specific personnel to be available on a 24/7 basis to respond to alerts

Sub-requirement 12.9.4: Provide appropriate training to staff with security breach response responsibilities

Sub-requirement 12.9.5: Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems

Sub-requirement 12.9.6: Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments

Again, to meet this requirement, it is important to have clarity in roles and responsibilities. Organizations must identify who is going to communicate to whom and how, implement a business continuity component, and meet any legal requirements for reporting. The plan should also identify who will be available to respond to alerts and must incorporate alerts from IDS, IPS, and file integrity monitoring systems. Auditors will be looking for a way to verify or observe that someone is monitoring and responding to these alerts. Importantly, the incident response plan should be tested annually. In addition, staff should be trained on security breach incident response roles and responsibilities.

Requirement 12.10
All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following:

Sub-requirement 12.10.1: Maintain a list of connected entities

Sub-requirement 12.10.2: Ensure proper due diligence is conducted prior to connecting an entity

Sub-requirement 12.10.3: Ensure the entity is PCI DSS compliant

Sub-requirement 12.10.4: Connect and disconnect entities by following an established process

Processors and service provider organizations must ensure that connected entities are PCI compliant, and these connected entities exercise as much due diligence as the processor or service provider organization itself.

How Ecora Software Can Help Organizations Ensure PCI Compliance

Ecora Software can help organizations demonstrate compliance to pass key 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, to network devices and firewalls, to mail servers, to application enablers, to 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 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, allows 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 tracking and monitoring access to cardholder data, for example, Ecora can generate a report that verifies events are being logged, including where the log is located, and whether the log is enabled. Other reports can identify all invalid system access attempts. Similarly, Ecora can show system-level changes, roles in the database, and all configuration data collected. These change reports can be run for all system components quarterly to identify all changes, or more frequently such as after any significant changes.

Importantly, once any Ecora report is run to assess compliance, issues can be resolved, and then the reports can be generated again to demonstrate compliance for auditors.

To be successful, an organization must demonstrate they have control of change in their environment. Organizations that use industry best practices, including the automated, 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 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 or +1 603.436.1616, 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.

ecora

2 International Drive, Suite 150 | Portsmouth, NH 03801 | p:877.92.ECORA 603.436.1616 | f:603.436.4344