ecora

WHITEPAPER

Using Automated, Detailed Configuration and Change Reporting to Achieve and Maintain PCI Compliance Part 2

An in-depth look at Payment Card Industry Data Security Standard Requirements 1, 2, 3, 4

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 standards, 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.

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 infrastructure 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.

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 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 large enough sample of firewalls, routers, wireless access points, databases, etc. to validate findings representative of the entire environment. Importantly, the more standardized the environment and the more clearly defined the configuration standards, the smaller the sample.

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 fairly broad at first glance, each requirement actually include extensive sub-requirements that make ensuring PCI compliance substantially more complex.

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

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

Firewalls provide the first line of defense for any computer network, and for networks on which cardholder data is stored, processed, and transmitted, they are vital to ensuring that information is secure. They validate only traffic meeting security parameters is granted access.

In fact, one of the underlying concepts of the PCI standard is segregating the network and systems involved with processing credit card data from the rest of an organization's IT infrastructure components. For this reason, firewall configuration standards are closely scrutinized during the course of an audit. Ideally, an organization has a solid change management process in place so that proposed changes to firewall and router configurations are thoroughly reviewed and the impact of the changes is understood. Auditors will verify that a formal change management process is in place for firewall configurations.

Requirement 1.1

Establish firewall configuration standards that include the following:

Sub-requirement 1.1.1: A formal process for approving and testing all external network connections and changes to the firewall configuration

Sub-requirement 1.1.2: A current network diagram with all connections to cardholder data, including any wireless networks

Sub-requirement 1.1.3: Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone

Sub-requirement 1.1.4: Description of groups, roles, and responsibilities for logical management of network components

Sub-requirement 1.1.5: Documented list of services and ports necessary for business

Sub-requirement 1.1.6: Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)

Sub-requirement 1.1.7: Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented

Sub-requirement 1.1.8: Quarterly review of firewall and router rule sets

Sub-requirement 1.1.9: Configuration standards for routers

In order to fulfill all elements of this requirement, it is critical that organizations update their network diagrams quarterly, documenting all connections to cardholder data, including any network systems that can be accessed wirelessly.

Organizations also need to ensure firewalls are in place at each Internet connection to protect internal systems from unauthorized access by traffic entering or leaving the DMZ. Auditors will be looking for evidence that such a configuration is in place.

Table 1. Domain Admins Group

Domain	User Name	User Full Name	User Account Expires	User Lockout	User Disable
SampleOrgDOMAIN	Administrator			No	No
SampleOrgDOMAIN	ecm_2	ecm_2		No	No
SampleOrgDOMAIN	PMPUser	PMPUser		No	No
TESTSRV4DOMAIN	a1	,		No	No
TESTSRV4DOMAIN	Administrator			No	No
TESTSRV4DOMAIN	as	1		No	No
TESTSRV4DOMAIN	cm_admin3	cm_admin3		No	No
TESTSRV4DOMAIN	ecm_2458000	ecm_2		No	No
TESTSRV4DOMAIN	ecm_3	ecm_3		No	No
TESTSRV4DOMAIN	ecora	ecora		No	No
TESTSRV4DOMAIN	gobbo	Gobbo		No	No
TESTSRV4DOMAIN	kfd	king for a day		No	Yes
TESTSRV4DOMAIN	tester	For Testing		No	No
DOMAIN-A	Administrator	Administrator		No	No
DOMAIN-A	ecora	ecora		No	No
DOMAIN-A	User_A1_B1	User_A1_B1		No	No
DOMAIN-B	Administrator			No	No
DOMAIN-B	ecora	ecora		No	No
DOMAIN-B	User_B1_A1	User_B1_A1		No	No
DOMAIN-C	Administrator			No	No
DOMAIN-C	ecora	ecora		No	No
ECORA	Administrator			No	No
ECORA	ecora	ecora		No	No
TESTSRVDOMAIN	db2admin	db2admin		No	No
TESTSRVDOMAIN	ecm_4	ecm_4		No	No
TESTSRVDOMAIN	ecora	ecora		No	No
TESTSRVDOMAIN	ecorapvm	ecorapvm		No	No
TESTSRVDOMAIN	PMPUser	PMPUser		No	No
MORDOR_NB	Administrator			No	No
MORDOR_NB	ecora	ecora		No	No

Ecora's Domain Admins Group Report fulfills PCI DSS 1.1.4, "Verify that firewall configuration standards include a description of groups, roles, and responsibilities for logical management of network components."

Auditors will also be looking for documentation that clearly shows the groups, roles, and responsibilities of employees who have access to an organization's physical network, particularly to firewall configuration settings, and the services and ports necessary for business, ideally with the absolute minimum number of ports accessible externally. Auditors should be able to view reports validating settings with actual data against an organization's stated policies.

In addition, an organization should be able to provide justification and documentation for available protocols, including any "risky" protocols. All traffic that touches cardholder data must be encrypted—encryption is absolutely paramount. For example, auditors will want to see evidence that only HTTPS, SSL, SSH, and VPN ports are open and this is the only type of traffic entering and leaving the network where cardholder data is stored, processed, or transmitted. Plus, because they can be vulnerable to threats from unauthorized users, it is important that organizations avoid protocols such as FTP whenever possible. Open FTP ports will likely lead to additional auditor scrutiny.

Rule sets control what enters and exits the network, and organizations should review current rule sets quarterly. Since auditors will look for evidence that a regular review is taking place, organizations should also document any meetings, discussions, or other interactions where rule sets are reviewed.

And, it is equally essential that an organization demonstrate configuration standards are in place for routers, as with firewalls.

Requirement 1.2

Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.

Clearly there are certain Internet segments that must be avoided, and an organization's router rule set must show that access to these segments is denied. Plus, as was the case with the firewall rule set, the router rule set should be updated regularly and documentation of the updates maintained.

Requirement 1.3

Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks.

This firewall configuration should include the following:

- Sub-requirement 1.3.1: Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)
- Sub-requirement 1.3.2: Not allowing internal addresses to pass from the Internet into the DMZ
- Sub-requirement 1.3.3: Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)
- Sub-requirement 1.3.4: Placing the database in an internal network zone, segregated from the DMZ
- Sub-requirement 1.3.5: Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment
- Sub-requirement 1.3.6: Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration
- Sub-requirement 1.3.7: Denying all other inbound and outbound traffic not specifically allowed
- Sub-requirement 1.3.8: Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)
- Sub-requirement 1.3.9: Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network

This requirement and its sub-requirements clearly state that any servers that are accessible externally should not have direct connections to system components where cardholder data is stored, such as application servers and databases. Databases that house cardholder data should be placed in an internal network zone, to ensure a level of separation between databases and the DMZ. Firewall configurations should limit inbound Internet traffic to Internet protocol (IP) addresses; any external traffic should only communicate with servers inside the DMZ. In fact, only traffic required for the cardholder data environment should flow through these segments of the network, and all other inbound or outbound traffic should be denied access. Any traffic not specifically related to the business should not be allowed. There should be no open ports beyond those necessary for encrypted communication; having "unnecessary" open ports will raise questions in an audit.

In addition, perimeter firewalls should be deployed between the wireless network and the cardholder data environment to deny access to any traffic from the wireless environment; if it is not required for credit card processing activity, the wireless network should be completely separated from network components related to cardholder data. Auditors will look closely at wireless security.

Organizations should also install personal firewall software on all laptops and other PCs that can access an organization's network, especially if they will access any system linked to the cardholder environment.

It is also essential that firewalls support stateful inspection or dynamic packet filtering functionality. Auditors sometimes run NMAP on all TCP/IP ports to validate that expected traffic is going in the right direction, and it is a good idea for organizations to run NMAP before auditors do.

Finally, router configuration files should be synchronized so that running configuration files match the on-disk configuration. Auditors will reboot routers and firewalls to verify that the configuration files are in-sync.

Requirement 1.4

Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).

- Sub-requirement 1.4.1: Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic
- Sub-requirement 1.4.2: Restrict outbound traffic from payment card applications to IP addresses within the DMZ

Again, it is essential to prevent any direct public access between the system components that store cardholder data and any external networks and the Internet. To meet this requirement, organizations should implement a DMZ (as stated in previous requirements) that will screen inbound and outbound Internet traffic to protect cardholder data.

Organizations should also restrict outbound traffic related to applications and databases where cardholder data is stored to IP addresses within the DMZ. Again, separation is essential. It should be common sense that no external connection from the Internet should connect directly to any internal system components, whether application servers, databases, or some other element.

Requirement 1.5

Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).

In addition to restricting traffic between internal and public systems, organizations should also deploy techniques such as IP masquerading to hide IP addresses. The ideal approach to satisfy this requirement is to implement RFC 1918, with port address translation and network address translation.

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

Anyone with the desire to threaten a network—whether from outside an organization or from within—begins by using vendor-supplied default passwords and other default settings, which are often common knowledge. Organizations should evaluate all PCI-related IT components—including firewalls, routers, switches, database servers, directories, and applications—to generate lists of the default passwords, user IDs, and passwords. Then, they should ensure all default system passwords have been disabled and service accounts have either been disabled or there is a justifiable reason for them to exist. This can be a challenge with the number of systems and components involved—the more components, the more validation required.

Requirement 2.1

Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol [SNMP] community strings, and elimination of unnecessary accounts).

Sub-requirement 2.1.1: For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

For wireless environments in particular, security is essential and levels of auditor scrutiny are high. Organizations should limit the use of wireless technology, especially WEP security, in networks and systems where cardholder data is processed, transmitted, or stored. If an organization relies on wireless technology and there is no way to separate the wireless and cardholder environments, more sophisticated encryption technologies—such as WPA and WPA2—should be deployed. In addition, the default SSID and SNMP community strings on access points should be changed. One of the first things an auditor will look for is the "public" default community string.

Requirement 2.2

Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

Sub-requirement 2.2.1: Implement only one primary function per server (for example, web servers, database servers); DNS should be implemented on separate servers

Sub-requirement 2.2.2: Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)

Sub-requirement 2.2.3: Configure system security parameters to prevent misuse

Sub-requirement 2.2.4: Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers

In this requirement, The PCI Security Standards Council is urging organizations to undertake a system-hardening process. Organizations that have already adopted best practices from SANS, NIST, or CIS will be well-positioned for meeting PCI requirements.

As part of the system-hardening process, PCI requires a clear separation of server functionality. This means there should only be one primary function per server. If, for example, an organization uses a DNS server, all it should be doing is DNS; organizations should resist the temptation to reduce expenses or operating costs by combining server functions.

As was the case with Requirement 1, which requires unnecessary and insecure protocols to be disabled on firewalls and routers, this requirement mandates organizations do the same with systems. Whether an organization runs Windows, Unix, or Linux, only ports that are absolutely necessary should remain open. Organizations should also ensure that all unnecessary functionality, such as scripts, drivers, features, subsystems, etc., is disabled or removed. Again, the only functionality deployed on these systems should be directly related to processing cardholder data.

In addition, system security parameters should be configured to prevent misuse. To verify this requirement is met, auditors will interview system administrators and security managers to confirm their knowledge of security parameters in the operating system, database, and web server environment, and the statements of all those interviewed are consistent.

Requirement 2.3

Encrypt all nonconsole administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other nonconsole administrative access.

To harden systems and encrypt nonconsole administrative access, organizations should eliminate Telnet and use SSH, VPN, or SSL/TLS technology.

Requirement 2.4

Hosting providers must protect each entity's hosted environment and data.

This requirement specifically targets service providers and is designed to ensure the accounts and data of each of their clients is separated. There should be absolutely no crossover between clients' systems, databases, applications, etc. so no cross-account hacking can take place.

Ecora's Baseline Comparison Report fulfills PCI DSS 2.2.c, "Verify that system configuration standards are applied when new systems are configured."

Requirement 3:
Protect stored cardholder data.

Simply put, all cardholder data should be encrypted. This will ensure information is protected even if the security tools and techniques outlined by other PCI requirements are circumvented. It is important, however, that organizations understand how encryption keys should be managed, as well as how, and what, cardholder data can be stored.

Requirement 3.1

Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.

There should be clearly defined limits on the quantity and length of time cardholder data is stored. In fact, it is ideal if an organization can eliminate the need to store cardholder data at all; although for most, this would not be realistic.

Consider, for example, the case of an organization with an e-commerce site. Will customers be satisfied if they have to re-enter credit card information every time they visit? To meet these requirements, organizations should develop a clear and comprehensive policy regarding stored cardholder data: documenting business requirements, why data is stored and for how long, how it will be disposed, and who is authorized to touch the data, for example. In developing this policy, organizations should look to both their compliance team and their legal counsel. Auditors will be looking for a sound policy document that adheres to legal and regulatory requirements.

Requirement 3.2

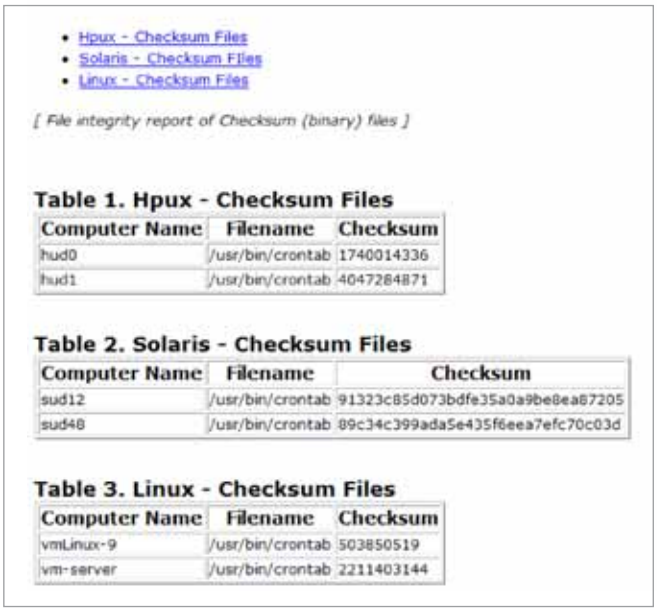
Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following:

Sub-requirement 3.2.1: Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data

Sub-requirement 3.2.2: Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions

Sub-requirement 3.2.3: Do not store the personal identification number (PIN) or the encrypted PIN block

It is good security practice to keep authentication and authorization data separate, and organizations can accomplish this by ensuring that they are not stored in the same physical area. In addition, the information retrieved from a card's magnetic stripe should not be stored together; it should be stored in separate systems, transaction logs, history files, trace files, etc. Also, card-validation codes and PIN numbers should not be stored at all. Auditors should discover no instance of this data on your systems.



- Hpux - Checksum Files
- Solaris - Checksum Files
- Linux - Checksum Files

[File integrity report of Checksum (binary) files]

Table 1. Hpux - Checksum Files

Computer Name	Filename	Checksum
hud0	/usr/bin/crontab	1740014336
hud1	/usr/bin/crontab	4047284871

Table 2. Solaris - Checksum Files

Computer Name	Filename	Checksum
sud12	/usr/bin/crontab	91323c85d073bdfe35a0a9be8ea87205
sud48	/usr/bin/crontab	89c34c399ada5e435f6eea7efc70c03d

Table 3. Linux - Checksum Files

Computer Name	Filename	Checksum
vmLinux-9	/usr/bin/crontab	503850519
vm-server	/usr/bin/crontab	2211403144

Ecora's Checksum Report fulfills PCI DSS 3.5.2, "Examine system configuration files to verify that cryptographic keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys."

Requirement 3.3

Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).

Organizations need to implement very specific guidelines about what cardholder data can be displayed, on receipts, for example. The fewer digits displayed, the better.

Requirement 3.4

Render PAN, at a minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

- Strong one-way hash functions (hashed indexes)
- Truncation
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key management processes and procedures

Sub-requirement 3.4.1: If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.

The PAN should be unreadable anywhere it is stored, and organizations can use a number of technologies to ensure this is the case. The best option is strong cryptography, such as Triple DES 128-bit or AES 256-bit encryption. Plus, access to encryption information should not be stored in a directory; it should be stored separately.

Requirement 3.5

Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.

Sub-requirement 3.5.1: Restrict access to keys to the fewest number of custodians necessary

Sub-requirement 3.5.2: Store keys securely in the fewest possible locations and forms.

To demonstrate encryption keys are protected, organizations should maintain a list of users who are allowed to access keys. It is important to update the list and ensure access to it is restricted. In addition, there should be a limit to the number of individuals who have access to the keys, and keys should be stored in as few places as possible.

Requirement 3.6

Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:

Sub-requirement 3.6.1: Generation of strong keys

Sub-requirement 3.6.2: Secure key distribution

Sub-requirement 3.6.3: Secure key storage

Sub-requirement 3.6.4: Periodic changing of keys (as deemed necessary and recommended by the application; preferably automatically and at least annually

Sub-requirement 3.6.5: Destruction of old keys

Sub-requirement 3.6.6: Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)

Sub-requirement 3.6.7: Prevention of unauthorized substitution of keys

Sub-requirement 3.6.8: Replacement of known or suspected compromised keys

Sub-requirement 3.6.9: Revocation of old or invalid keys

Sub-requirement 3.6.10: Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.

Organizations should implement stringent key-management processes, and have well-documented access key controls. In addition to ensuring keys are strong and secure, they should be changed periodically and old or compromised keys should be revoked and/or destroyed, and not just when there is a security breach. The use of dual-control keys, which require two or more individuals to each know a portion of the key (ensuring no one individual can reconstruct a key themselves), can help ensure security.

Solid change management and control processes can ensure key management processes are being followed.

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

This requirement ensures that any traffic going over the public Internet, whether into or out of an organization's website, is encrypted. Organizations may meet this requirement using a number of technologies, including Secure Socket Layer (SSL), IPSec, WPA, and WPA2.

Requirement 4.1

Use strong cryptography and security protocols such as secure sockets layer (SSL)/transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Sub-requirement 4.1.1: For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS.

Data should be encrypted during the transmission process to and from public networks. Auditors will be looking, for example, to be sure that an organization's URLs are HTTPS and that they're using protocols such as SSH.

If the cardholder processing infrastructure and the wireless network can not be physically separated, wireless networks transmitting cardholder data should use WPA or WPA2 technology, IPSEC VPN, and SSL/TLS. The use of WEP should be avoided whenever possible to ensure optimal security.

Requirement 4.2

Never send unencrypted PANs by e-mail.

Organizations should have a clearly defined policy stating that encrypted PANs should never be distributed via e-mail. Auditors will interview an organization's employees to ensure no system component sends PANs in encrypted form.

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 with a tremendous savings in time and resources, but this approach only works if an organization has the ability to identify and report on the entire infrastructure. Ecora software 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 software discovers an organization's critical systems and collects configuration data—including security-related data such as credentials, permissions, access controls, and more. Importantly, the software enables organizations to generate reports to assess controls and identify who has access to which systems and data, validating that the current situation matches expected results.

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, from which ports are opens to what hardware and services are up and running. Organizations can drill down further into this information to see exactly how components are configured. Our CheckPoint module, for example, enables organizations to collect firewall-related information about groups and roles, administrative lists, network translation tables, and more.

To be successful, an organization must demonstrate they have control of change in their environment, and any processes put in place to ensure a successful PCI audit can have far-reaching implications 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 or +1 603.436.1616, email sales@ecora.com, or visit us on the web at www.ecora.com.

About Ecora

Proven in nearly 4,000 worldwide customer sites, Ecora's leading enterprise-wide audit and compliance management solutions are designed to reduce the time and costs associated with managing IT configuration controls, for enhanced infrastructure security. Ecora provides automated, centralized solutions to collect, analyze, and report on the most in-depth, multi-platform configuration information across enterprise operating systems, applications, databases, and networking devices. Ecora works to optimize IT environments and delivers an immediate return on investment. For more information about Ecora, visit www.ecora.com.

ecora

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