



**Network Configuration  
Management and PCI**

Deploying network configuration and  
change management technology to  
support and ensure PCI compliance



When information comes together,  
your world moves ahead.

## Introduction

Every day, millions of people and thousands of businesses around the world rely on credit card transactions to purchase everything from a cup of coffee at their local coffee shop, to a visit to their doctor's office, or a relaxing dinner after a long day's work. When handing over a credit card, a person expects that his or her personal information is safe and secure. Unfortunately, in recent years, the credit card and personal information of millions of people has been exposed unnecessarily because companies have not taken the necessary steps to protect and secure their networks, and ultimately—their businesses and customers.

The Payment Card Industry (PCI) Data Security Standard is a set of data security requirements that apply to any entities that store, process, or transmit credit card information. Major credit card companies—including Visa, MasterCard, American Express, Diner's Club, and Discover Card—created this standard to ensure that merchants and service providers keep credit card information secure.

Organizations validating their compliance with the PCI requirements help safeguard cardholder data, as well as enhance their reputations among their customers and partners as a safe place to do business. All organizations, whether they support card-issuing or acquiring activity, must undergo an annual verification process to validate compliance with the PCI security requirements defined by the PCI Security Council specification.

The traditional approach to securing, documenting, and auditing network infrastructure has been a mix of ad hoc manual processes, homegrown tools, and vendor-specific element management consoles. This has proven resource-intensive and error-prone, leading to weakened security postures and, often, a failure to document the network and its change history.

It is simply not enough to spot check and report on compliance; organizations also must be able to demonstrate how they are complying with the PCI Standard. Failure to comply, or to prove compliance, can have a range of implications, including:

- Diminished perception in the marketplace
- Financial penalties
- Increased transaction fees
- Being barred from processing credit card transactions

In addition, for most organizations, the issue of compliance extends to internal requirements that are important to the way an organization functions.

More specifically, a company must define its policies and procedures that govern how it operates—including limits on information access, change requests, approvals, and ultimately, how adherence is tracked and verified.

Industry, corporate, and regulatory requirement concerns have made compliance a top-of-mind issue for executives and the companies they lead. In fact, a recent study by SecurityCompliance.com indicates that 73 percent of companies are realigning their organizational structures to better respond to compliance pressures, and AMR Research recently stated that “compliance spending in 2006 will reach \$27.3 billion, with \$6 billion (or 22 percent) allocated to the Sarbanes-Oxley Act. Spending will climb even higher in 2007, with companies devoting \$28 billion to compliance initiatives.”

This document reviews the requirements of the PCI Standard that impact any entity that stores, processes, or transmits credit card information. It also discusses how EMC® VoyenceControl™ can help organizations ensure network compliance with internal and PCI requirements, and highlights how such organizations can benefit from VoyenceControl.

Please note: This document is designed to provide general information only and is not intended to be viewed as legal advice.

## Supporting an Organization’s Compliance and Security Management Strategy

Two fundamental goals form the basis for most efforts to ensure compliance. Organizations want to:

- Eliminate exposure to legal and business risk to protect themselves, their employees, and their customers
- Implement a compliance policy that protects their entire infrastructure and is continuous and comprehensive—and effective

However, realizing these goals is not without challenges. The most significant challenge can be the resources required to undertake a compliance initiative. The ideal is to leverage existing financial, human, and technological resources, and look to automated processes whenever possible to achieve compliance goals.

Core to PCI compliance mandates is to ensure that only authorized personnel access or modify critical information. As such, most compliance initiatives have focused on securing and documenting the applications, databases, and servers. They often overlook the role the network. If the network is not secure, then unauthorized access can be made through infrastructure vulnerabilities—negating any efforts on the servers, applications, or databases.

The best strategy: Apply automated network configuration and change management technology that supports and enforces an organization’s defined processes and policies to ensure and prove compliance with industry, legal, regulatory, and internal requirements.

VoyenceControl is an automated compliance, change, and configuration management solution that delivers industry-recognized best practices, a collaborative network infrastructure design, controlled change processes, network device and service configuration transparency, and compliance with corporate and regulatory requirements—to enable organizations to ensure the security, availability, and operational efficiency of their networks.

VoyenceControl provides vital support for an organization’s compliance and security management strategy, with the critical tools needed to ensure and demonstrate continual network compliance with defined policies, standards, industry requirements, and government regulatory requirements across network and change management processes.

## Achieving Compliance

Although the PCI Standard outlines the requirements organizations must meet, it does not detail how to achieve compliance with its requirements—for example, what policies organizations must implement on which devices or applications, or what organizational processes or controls organizations should implement.

To achieve compliance, many organizations adhere to the framework outlined by either the Committee of Sponsoring Organizations of the Treadway Commission (COSO) or the IT Infrastructure Library (ITIL). COSO is a voluntary, private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. Today, the SEC recognizes the COSO framework as the official framework for establishing internal controls over financial reporting.

Control Objectives for Information and Related Technology (COBIT) is the IT-specific component of COSO's framework. It provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes, and best practices to help them maximize the benefits of information technology in general, while developing appropriate IT governance and control.

### **COBIT recommends that organizations:**

- Implement change control monitoring/auditing tools and a change management system
- Document and implement preventive controls and procedures; defining who has access to what type of information, for example
- Document and implement detective controls
- Document change management workflow approval processes
- Document and report all unauthorized changes
- Provide accurate auditing of authorized changes as they relate to approved change management workflow processes

## **ITIL**

ITIL provides a standard framework of best practices intended to help enterprises manage their day-to-day operations efficiently and effectively to ensure that the IT infrastructure meets service-level agreements between IT and its customers.

## Reaching the Goal—Compliance Assurance

To comply with industry and regulatory—and to prove compliance to auditors—many organizations must make changes to their network infrastructures and process. According to Amer Deeba, vice president, strategic alliances for Qualys, in an article from the SC Magazine, “Vulnerabilities are discovered on a daily basis, and a continuous assessment and remediation process on a given network becomes a requirement to maintain a strong security posture.” He adds: “PCI provides a best-practices framework to secure an infrastructure and protect customers’ sensitive data. Typically such a process has to be audited on a regular basis in order to make sure that these best practices are met.”

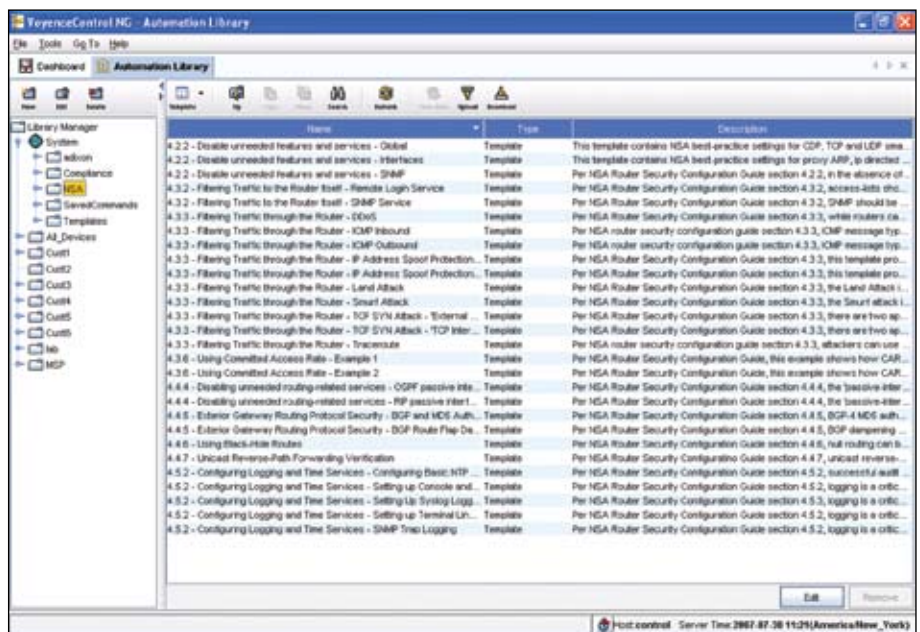
PCI compliance represents more than just a “spot check,” and the goal for organizations must be compliance assurance. VoyenceControl is uniquely positioned to help customers achieve this goal. Compliance assurance entails a number of steps, and VoyenceControl is the only automated network configuration and change management solution that supports organizations through each step.

### Step 1: Set Policies

To realize compliance assurance, organizations must identify vulnerabilities and create policies to address those vulnerabilities, as well as define what permissions are granted to users of the system.

#### How VoyenceControl helps:

- Creates multi-vendor policies that help enforce industry and regulatory compliance
- Limits access to change configuration privileges with role-based security
- Provides templates that meet NSA Guidelines for access control lists, interface settings, and secure configuration best practices



## Step 2: Ensure Policies Are Enforced

Organizations must maintain rigorous adherence to defined policies and procedures, control change with role-based processes and workflow approvals, and enable rapid remediation in response to threats.

### How VoyenceControl helps:

- Configuration through templates ensures that changes are performed in a predictable and consistent manner
- A workflow/approval process ensures that changes can be audited and validated against policies for compliance at the time of change—prior to activation
- External or direct devices changes are automatically detected and proactively audited to ensure compliance with the defined policies

## Step 3: Remediate Policy Violations

Although organizations need to demonstrate that they meet standards and policies on demand, they also have to show how violations are recognized, audited and remediated—in real time.

### How VoyenceControl helps:

- All changes in the infrastructure are identified automatically and audited for compliance
- Provides automated scheduling or “one-click” remediation to bring non-compliant devices into compliance

## Step 4: Prove that Policies Are Enforced across the Infrastructure

Implementing standards and policies across the entire infrastructure—and not just at the device level—is essential. Organizations must create a defined structure for change management processes, as well as produce reports that can prove continuous compliance, as well as identify any device and process violations.

### How VoyenceControl helps:

- Provides reporting on demand to demonstrate continual policy and regulatory compliance
- Enables realtime and historical reporting capabilities—across device compliance and change management process adherence



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

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via pub information.

PCI DSS Requirements	Reports / Links	Review Comments												
<p><b>2.1.1 Always change vendor-supplied defaults before installing a system on the network</b> (for example, include passwords, single network management protocol (SNMP) community strings, and elimination of unnecessary accounts).</p>	<p>Reports / Links</p> <ul style="list-style-type: none"> <li>Credential User Report</li> <li>Communication Mechanism Report</li> </ul> <table border="1"> <thead> <tr> <th>Compliance Item</th> <th>Compliant</th> <th>Not Compliant</th> </tr> </thead> <tbody> <tr> <td>Default Passwords - Cisco</td> <td>2772</td> <td>23</td> </tr> <tr> <td>Default SNMP - Cisco</td> <td>2794</td> <td>1</td> </tr> <tr> <td>No local accounts - Cisco</td> <td>2200</td> <td>595</td> </tr> </tbody> </table>	Compliance Item	Compliant	Not Compliant	Default Passwords - Cisco	2772	23	Default SNMP - Cisco	2794	1	No local accounts - Cisco	2200	595	<p>5/3/07 - Matt Clark Updated default passwords policy to include FWs from latest IOS</p> <p>8/3/07 - Matt Clark Reviewed policies are up to date</p>
Compliance Item	Compliant	Not Compliant												
Default Passwords - Cisco	2772	23												
Default SNMP - Cisco	2794	1												
No local accounts - Cisco	2200	595												
<p><b>2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Tenable</b></p>	<p>Reports</p> <ul style="list-style-type: none"> <li>Inventory Report - Wireless Devices</li> </ul> <table border="1"> <thead> <tr> <th>Compliance Item</th> <th>Compliant</th> <th>Not Compliant</th> </tr> </thead> <tbody> <tr> <td>Strong WEP</td> <td>802</td> <td>72</td> </tr> <tr> <td>Encryption</td> <td>407</td> <td>468</td> </tr> <tr> <td>No Default SSID</td> <td>407</td> <td>468</td> </tr> </tbody> </table>	Compliance Item	Compliant	Not Compliant	Strong WEP	802	72	Encryption	407	468	No Default SSID	407	468	<p>5/3/07 - Matt Clark Reviewed policies are up to date</p> <p>8/3/07 - Matt Clark Updated 'No Default SSID' to include the Aruba devices</p>
Compliance Item	Compliant	Not Compliant												
Strong WEP	802	72												
Encryption	407	468												
No Default SSID	407	468												

Comprehensive compliance assurance is critical for organizational success, and VoyenceControl enables organizations to achieve compliance assurance, delivering the change management process essential to any compliance initiative, managing compliance to policies in real time, and delivering definitive proof of regulatory compliance across the network and change management process.

PCI Requirements	How VoyenceControl Helps
<b>Build and Maintain a Secure Network</b>	
<b>Requirement 1.0</b> Install and maintain a working firewall configuration to protect cardholder data	VoyenceControl is a vendor-neutral solution for managing the configurations of network infrastructure devices of all models and types including firewalls. VoyenceControl enables strong adherence to defined change management processes, captures the who, what, when, why, and how of every change. In addition, VoyenceControl provides out-of-the-box samples allowing organization to define firewall and network device configuration standards along with realtime policy management and auto-remediation scheduling when violations are present.
<b>Requirement 2.0</b> Don't use vendor-supplied defaults for passwords and security parameters	Configuration templates, design wizards, and compliance standards are used to ensure that all network device configurations adhere to security policies.
<b>Protect Cardholder Data</b>	
<b>Requirement 3.0</b> Protect stored cardholder data	Critical network configuration information is stored securely in a central repository.
<b>Requirement 4.0</b> Encrypt data sent across public networks	All network configuration data is sent via SSL or SSH. Compliance policies can be constructed to ensure maximum security settings are being used on links that transmit cardholder data.
<b>Maintain a Vulnerability Management Program</b>	
<b>Requirement 6.0</b> Develop and maintain secure systems and applications	VoyenceControl manages the configuration of routers, switches, firewalls, and other network devices. VoyenceControl allows IT professionals to quickly identify operating system (OS) management and OS version reporting utilizing configuration and hardware search features. This capability provides quick visibility into affected network devices running compromised OSs, and also can automate deployment of security patches and OS images.
<b>Implement Strong Access Control Measures</b>	
<b>Requirement 7.0</b> Restrict access by cardholder data by business need-to-know	The role-based user authentication model restricts device access and sensitive configuration data on a need-to-know basis to support your defined policies.
<b>Requirement 8.0</b> Assign a unique ID to each person with computer access	VoyenceControl is integrated with LDAP, TACACS/TACACS+, RADIUS, and native registry, allowing unique credentials to be imported and utilized within the system for device access and change auditing.
<b>Regularly Monitor and Test Networks</b>	
<b>Requirement 10.0</b> Track and monitor all access to network resources and cardholder data	VoyenceControl tracks and stores all user activity and network device configuration changes with appropriate user IDs. VoyenceControl also tracks and stores device changes made directly to the devices.
<b>Requirement 11.0</b> Regularly test security systems and processes	VoyenceControl's workflow, change management and compliance reporting provides the means to monitor, test, and ensure your defined security procedures and policies are adhered to.
<b>Maintain an Information Security Policy</b>	
<b>Requirement 12.0</b> Implement and maintain an information security policy	VoyenceControl's compliance standards allow security architects and engineers to define and enforce security policies across the entire network infrastructure, as well as aiding them in producing the documentation necessary to provide to an auditor.

## Conclusion

Companies need to fully understand how to approach PCI compliance as a long-term program to secure business activities. Addressing PCI requirements in a reactive mode yields quick, uninformed decisions that still may leave systems open to security breaches and substantial fines. Administrators must take network configuration seriously to circumvent internal and external data breaches. VoyenceControl's automated processes that audit and enforce predefined and easy-to-create configuration security standards and conduct realtime PCI compliance tests and remediations can greatly help reduce security risks, threats, and vulnerabilities.

As an independent company, Voyence was a Participating Organization of the Payment Card Industry (PCI) Security Standards Council. In October 2007, EMC acquired Voyence. Voyence will help influence the direction of PCI standards through active involvement in community meetings, provide advance review of drafts of standards and supporting materials, and continue regular dialogue with key stakeholders.

As a member of the Council, Voyence will be committed to the maintenance and ongoing evolution of the PCI Data Security Standard, while working to promote the broad industry adoption of the standard and providing the tools needed for companies to properly secure network devices.



**EMC Corporation**  
Hopkinton  
Massachusetts  
01748-9103  
1-508-435-1000  
In North America 1-866-464-7381  
[www.EMC.com](http://www.EMC.com)