PCI DSS Best Practices :
Simple Strategies for Achieving Compliance

Authored by: Dave Shackleford
Director of The Center for Policy & Compliance

January, 2009

Configuresoft

Security, Compliance and Control for the Virtualized World.

Table of Contents

Introduction

Since 2005, PrivacyRights.org has tracked over 245 million reported incidents where data records containing personal information such as Social Security numbers, account numbers, and driver's license numbers have been compromised due to security breaches.

Security breaches, such as the ones mentioned above, and the costs associated with those breaches have put increased pressure on organizations to achieve and maintain compliance with mandates such as the Payment Card Industry Data Security Standard (PCI DSS).

To do so, organizations must establish measurable controls that protect critical information assets – such as cardholder data in the case of PCI DSS – and put into practice a process that validates that these controls have been implemented and maintained over time.

Established in 2004, The Center for Policy & Compliance (CP&C) is comprised of security and policy experts, IT auditors, and early contributors to federal mandates and industry best practices who translate regulatory mandates, vendor recommendations, and industry best practices into advice and tools that IT organizations can easily implement as part of their goal of achieving compliance.

Is this Whitepaper for You?

The Center for Policy & Compliance (CP&C) has prepared this document for companies who are attempting to understand the broad-reaching implications of PCI DSS compliance, its ramifications on their organizations, and in particular, what is necessary to prepare for an upcoming audit.

Presented here is an in-depth look at exactly what the PCI DSS requirements are, plus advice from the CP&C on how to apply them to your company and IT environment. You'll also find knowledgeable insights on the best way to develop a plan that not only will help you immediately remediate non-compliance issues, but also help you increase audit readiness and establish longer term, continuous controls.

Based on the extensive knowledge of CP&C experts, this white paper will help you confidently answer each of the questions below and then implement a strategic, systematic process that will help assure ongoing PCI DSS compliance.

- Does my company need to comply with PCI DSS requirements?
- If so, are our current security policies and processes sufficient to assure compliance?
- If not, where are our systems vulnerable? What would be considered violations by a qualified auditing professional?
- If we are non-compliant according to the requirements of PCI DSS, how do we remediate the violations to become compliant today and remain so on a continuous basis?

Overview: The Complexity of Compliance

While many organizations have implemented many best practice security measures to protect critical information and IT infrastructure assets, this may not be enough to assure compliance with each regulatory, security and organizational policy guideline that a corporation is mandated to follow.

Why? Simply because the complexity of managing compliance and the associated challenges of security hardening are continually evolving and increasing every day.

→ Compliance is a multi-faceted challenge. The majority of corporations fall under the governance of more than one type of compliance mandate because of the wide array of government regulatory requirements, industry best practices, security, and internal operational policies in place today. In addition, all of these mandates – including PCI DSS as well as Sarbanes-Oxley (SOX), HIPAA, and GLBA – are continually evolving, placing increasingly greater real-time demands on IT organizations.

→ There are overlapping, yet unique requirements. While many of the requirements from the individual mandates overlap one another, there are, at the same time, a number of unique guidelines for each regulatory directive. PCI DSS, for instance, has several specific requirements because of its primary focus on cardholder data.

→ Compliance mandates are often open to interpretation. Many of the mandates can often seem ambiguous, with the requirements being interpreted differently from auditor to auditor, thereby making compliance even more difficult.

→ Organizations have multiple compliance "experts." Because the compliance mandates have been introduced over time and govern different areas within an organization, they have been addressed as they have arisen, typically by the department that is governed by the regulations. This has caused the need for knowledge experts in particular areas, such as finance or networking, who then become responsible for assuring compliance for a particular mandate. Therefore, silos of compliance experts have developed throughout the organization, resulting in redundant and sometimes inefficient efforts to bring the company into complete compliance.

→ Change is a given. While many organizations may conduct yearly or regularly scheduled audits, their IT infrastructure and information assets are changing rapidly, even minute-by-minute, creating a continual state of risk. This is particularly prevalent as IT organizations embrace virtualization, where the rate of change grows exponentially, with more systems, more applications, and more complexity creating greater risk.

→ Auditing metrics are more demanding. Lastly, the auditing, testing, and evaluation policies of compliance are becoming complex and more challenging, opening organizations up to greater risks of non-compliance and the associated financial penalties.

PCI DSS: Does Your Company Need to Comply?

Many companies think if they are compliant with such regulations as SOX and HIPAA, then they are most likely compliant with other standards such as PCI DSS. That may not be the case, as this mandate specifically applies to any organization involved with payment cardholder data.

What is the PCI DSS? The PCI DSS is a worldwide security standard that was established in 2004 by the Payment Card Industry Security Standards Council (PCI SSC). The standard, enforced by founding members American Express, Discover Financial Services, JCB International, MasterCard, and Visa, is a set of expansive technical and operational system requirements aimed at preventing credit card fraud, hacking and various other security vulnerabilities and threats.

Who needs to comply? Any merchant or service provider who accepts, captures, stores, processes, or transmits cardholder data, including software developers and manufacturers of applications and devices used in related transactions.

What are the requirements? The six areas of compliance are: the building and maintaining of a secure network; the protection of cardholder data; maintaining a vulnerability management program; implementing strong access control measures; regularly monitoring and testing of networks; and maintaining an information security policy. Within these areas, there are 12 specific requirements (see page5 for the full set of requirements).

What auditing is required? All merchants and providers who need to comply with PCI DSS requirements are required to do either an annual self-assessment questionnaire, or if the volume of transactions is six million or more a year, an annual onsite audit. In addition, quarterly network scans are required for all merchants. The annual on site audits must be performed by an independent Qualified Security Assessor (QSA), while the quarterly scans must be performed by an independent Approved Scan Vendor. Alternatively, an internal audit can be performed if signed by an Officer of the Company.

PCI Compliance: Difficult and Ongoing

"PCI (Payment Card Industry) compliance - a requirement for accepting credit card transactions — can be difficult. About 65% of global enterprises are still working on their PCI compliance initiatives.

But PCI compliance is an ongoing effort, not a bounded IT security project."

Forrester Research
September 2008

Is your organization in PCI DSS compliance? If your organization is in involved with cardholder data and you are uncertain as to whether you are in compliance, you can follow the steps outlined in this white paper. If you are non-compliant, you'll learn exactly where you are in violation and how to develop a compliance strategy.

The Four Steps to PCI DSS Compliance

At the heart of any compliance strategy is first an understanding of the nature and volume of risk that your organization faces, and then the development of an implementation plan that puts into place appropriate controls in order to manage the risks effectively.

With that understanding, the CP&C recommends four easy steps your organization can take in order to achieve PCI DSS compliance.

1. Discovery: The first step requires that you analyze your IT environment and gain visibility into the full extent of your IT operations.
2. Mapping: Once you have a full understanding of your IT infrastructure, you can then align your environment with PCI DSS guidelines.
3. Assessment: This step will help you find out exactly where you are non-compliant by determining what controls might be deficient or missing.
4. Remediation: Here you will be presented with very specific options as to how to fix or mitigate the risk of non-compliant issues and develop an ongoing compliance strategy.

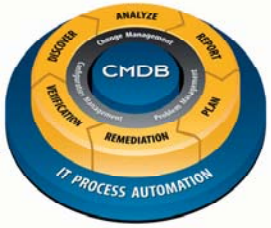
By implementing each of these four steps, your organization will be able to understand the most critical requirements of PCI DSS and have a comprehensive strategy for ensuring long-term, continuous compliance.

Step One: Discover the Assets in Your IT Environment

Before you can verify your compliance with the PCI DSS requirements, you need to have a thorough understanding of what your IT environment looks like, including its networks, servers, workstations, applications.

Your organization may already do this in a variety of ways, through a network scan, an asset management tool, a manually maintained spreadsheet, or some other process that provides visibility into your infrastructure.

Configuresoft, for example, has a solution called the Enterprise Configuration Manager (ECM) that collects tens of thousands of asset, security and configuration data settings from each networked Windows, UNIX and Linux server and workstation in an organization's environment. ECM then stores the data in a centralized Configuration Management Database (CMDB) and allows IT to have complete visibility into its infrastructure at any given time.



Configuresoft ECM collects information about the assets in your environment and stores it in a centralized database, making it easy for you to gain a comprehensive look at your entire IT environment.

However you gain visibility into your IT infrastructure, it's important to make sure that your view is complete and comprehensive so you will be able to identify any area of PCI DSS vulnerability and potential risk.

Step Two: Map PCI DSS Requirements to Your Environment

With a comprehensive view of your IT infrastructure, you will be able to determine, from a broad perspective, whether your company is in compliance.

The PCI DSS requirements, as established by the PCI SSC, are:

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and application
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

With the guidelines above, you can now look at your environment and determine which of your specific assets fall within the governance of the PCI DSS requirements.

For instance, as you review your list of servers, some of them may store cardholder data and will be subject to the PCI DSS requirements. Other servers may be used for entirely separate purposes and therefore will not under the mandates of PCI DSS.

With this information in hand, you can then document, on a per asset basis, whether that particular asset is in scope for PCI DSS, and procedure to the next step, which is assessing your compliance.

Step Three: Assess Your Level of PCI DSS Compliance

Now that you are aware of what assets in your IT environment fall under the guidance of the PCI DSS requirements, the next task is to figure out how to apply the those requirements to your environment and find specific issues of non-compliance.

You can do this process manually, or you can use a tool such as Configuresoft's PCI DSS Compliance Checker, which is a free utility that can provide you with this kind of information through one easy assessment. With its simple point-and-click interface, this downloadable utility (http://compliancechecker.configuresoft.com) will perform a real-time analysis of your systems and how they are configured in relation to PCI DSS.

Developed under the guidance of CP&C experts, the Compliance Checker comes with a PCI DSS template that is based on the rules specified by the PCI SSC and controls best practices from the Center for Internet Security (CIS) and NIST.

Because of its focused nature on PCI DSS, Configuresoft's Compliance Checker can save your organization hours of tedious legwork. Each time you run the tool, it automatically maps your environment against the most critical requirements, assessing your vulnerability management program, the security of your network, what access control measures you have in place, and how your monitor and test your networks.

Once the process is complete, the Compliance Checker provides you with specific recommendations and step-by-step strategies as to how to address any required actions, advising you on how best to bring your environment into compliance.

With the Compliance Checker, you will also have access to a knowledge base of remediation advice from CP&C experts.

Step Four: Remediate Your Environment

Once you've run a utility like the Configuresoft PCI DSS Compliance Checker and discovered your environment's vulnerabilities and risks, you will be able to develop a strategy for remediation, with typically two options for achieving compliance.

The Manual Remediation Option

With a list of the specific PCI DSS violations you discovered in the previous step, you have the option to assign a team of IT resources to the task of fixing each objection, one by one. This alternative, however, has a few drawbacks to consider:

- Because industry regulations such as PCI DSS tend to be technically rigorous, the exact duration of manual remediation is unpredictable. Depending on the degree of non-compliance, the process may be simple and uncomplicated, with fixes completed quickly. However, if the violations are more extensive– for instance, spanning several servers – a manual remediation plan could be a lengthy process, requiring many hours of labor that would typically assigned elsewhere.

> *"Auditing is not a singular, one-time event. We must have continuous control over our audit and compliance initiatives and be ready for an audit at a moment's notice."*
>
> **TSYS**

- Additionally, while comprehensive, the Compliance Checker is much like an audit in that it is a snapshot of a moment in time. It is a given that after you initially run the Compliance Checker, your environment will change, whether because of the implementation of a patch, a new user being added, or even updated PCI DSS requirements. The fixes that your team sets out to make, therefore, may no longer be valid and it will be necessary to repeat continually the Compliance Checker and the manual remediation process in order to keep up with your ever-changing environment.

> *"Since we require our customers to present their credit cards when they rent a car, it is important that we safeguard the sensitive data contained on those cards. Using ECM helps us meet the PCI DSS compliance requirements through the use of automated rules to regularly track and monitor access to network resources and cardholder data."*
>
> **Dollar Thrifty**
> **Automotive Group, Inc.**

- The final consideration is that because of the nature of change – in that it is continual and spread throughout your IT organization – a manual fix is typically error prone, increasing not only your security risks, but making it more difficult, if not impossible, to ensure full compliance on a continual basis. Because of these potential drawbacks, the manual remediation option often ends up being a costly endeavor for many IT organizations.

A Comprehensive Solution

The most effective way to ensure compliance is with a best-in-class solution such as Configuresoft's ECM, which not only takes away the guess work of whether or not you're in compliance, but it also ensures immediate compliance today and well into the future.

The advantages of using a solution such as ECM for achieving PCI DSS compliance are:

- You'll have checks and controls (such as access control, audit control, and automated access change monitoring) that automatically evaluate the configuration of your environment in relation to the most critical PCI DSS requirements.

- You'll have an automatic remediation process that fixes PCI DSS non-compliant system configurations across the IT Infrastructure (in both physical and virtual environments), increasing your organization's ability to consistently meet its PCI DSS requirements.

- In addition, your organization will have the ability to perform not only PCI DSS remediation, but also other applicable compliance mandates (such as SOX, GLBA, and HIPAA), allowing for a continuous state of IT audit readiness.

- Your organization will also be able to centralize PCI DSS accountability and responsibility by centralizing the assessment, reporting, remediating, and auditing across heterogeneous operating systems with a single role-based solution.

> *"ECM's out-of-the-box compliance templates, intuitive interface and speed of implementation help us comply with requirements such as HIPAA, GLBA, Sarbanes-Oxley and PCI DSS to name just a few."*
>
> **Greg Allender**
> **Director of Global Information Security**
> **Convergys**

Cost Saving Realized Using Configuresoft PCI DSS Solution

PCI DSS Security Requirement	Estimated Manual Hours	Automation Hours	Time Savings with ECM	How ECM Solved
2.2 Configuration Management	400	2	398	Assures configuration standards and addresses all known vulnerabilities based on NIST guidance
5.1/5.2 Anti Virus & Anti Spyware	16	2	14	Assures proper configuration of security settings, services, AV & desktop firewalls
6.1 Patch Management	120	2	118	Assesses, delivers and verifies security bulletins (patches)
6.3/6.4 Application Discovery & Control	120	2	108	Continuously discovers software/application inventories & stores details
8.5 User Accounts & Authentication	40	2	38	Ensures proper user authentication and password management

Total Time Savings:	**99%**
Estimated Cost Savings:	**$150K***
Estimated Cost Savings Over 3 Years:	**$450K***

* ROI calculator presumes a $100K per year IT staff salary and a manual savings per Quarter.

While manual remediation may seem like the optimal choice initially, the drawbacks can be quite costly and in the end, an automated solution may be more effective and cost-efficient.

In fact, as you can see in the chart here, companies that use ECM for PCI DSS compliance have reported up to a 99% reduction in IT audit costs because of the solution's automated compliance enforcement.

Conclusion

Although PCI DSS is an excellent standard that is based upon best practice security guidelines, the goal of implementing any set of security controls is to monitor for change on a continuous basis, because simply put, compliance is not a snapshot in time.

Compliance, therefore, has become a painstaking and often burdensome necessity for any IT organization. With each mandate – whether industry, government, or simply a best operational practice ¬ it is important that your organization has a broad-reaching plan that is reliable, repeatable, and durable enough to withstand security vulnerabilities and required audits on a real-time basis.

In order to avoid the penalties of non-compliance – including financial fines, merchant restrictions, and the loss of consumer trust – the CP&C recommends organizations use tools like Configuresoft's Compliance Checker and ECM in order to achieve and maintain continuous compliance.

.

About Configuresoft

Configuresoft, the world's leading enterprise server configuration management provider, delivers the Configuration Intelligence® that brings automation and intelligence to IT operations. Hundreds of organizations, including 13 of the world's 25 largest companies, rely on Configuresoft to effectively and efficiently manage the complexity of today's physical and virtualized IT environments. Configuresoft's team of security and policy experts ensures continuous compliance with regulatory requirements such as Sarbanes-Oxley and industry standards such as PCI DSS, and Microsoft and VMware Hardening Guides.

More about the Center for Policy & Compliance

The CP&C regularly researches and delivers productized security, regulatory, and operational compliance knowledge via Configuresoft's Compliance Toolkits. Each toolkit consists of a set of rule-based templates, reports, and dashboards that easily plug into Configuresoft's ECM to ensure security and operational compliance within a focused area, such as PCI DSS.

Configuresoft
7450 Campus Drive
Colorado Springs, CO 80920
USA

1-719-447-4600 • 1-888-447-2220
www.configuresoft.com • sales@configuresoft.com

Configuresoft