



The Best PCI Audit of Your Life: Are You Ready?

Ben Rothke, CISSP PCI QSA

v1.0

Monday, July 21, 2008

www.lumension.com

© Copyright 2008, Lumension Security



Table of Contents

Introduction	2
The PCI Audit	2
Using a Framework for Security	3
SCAP	4
Pre-assessment Analysis	5
Reducing PCI Scope	6
Better Luck Next Time	6
Get Management Commitment	6
Lumension’s Security Suite – A Way to Get You There	6
Vulnerability Management	7
Endpoint Protection.....	7
Enterprise Data Protection.....	7
Compliance Management	7
Lumension Security Suite	7
Conclusion	9
About the Author	9



Introduction

Insanity is colloquially defined as doing the same thing over and over again, expecting a different result. For too long, corporations have had dealt with regulatory requirements in a rather insane manner. It goes something like this:

- Regulation/standard released
- Struggle to comprehend and digest
- Delay implementation
- Call in consultants to fix
- Answer all the checklists
- Spend more money
- Barely achieve the low-bar of compliance

One would think that after the colossal spending from Sarbanes-Oxley, companies would take a more formal approach to compliance. But two years of experience with PCI DSS (Payment Card Industry Data Security Standard) shows that companies are still using the same compliance strategy over and over again, and in some cases, still lying to their auditors and management.

This compliance insanity has to stop. Far too much money is spent, far too little ROI, and even less effective security is gained via this broken process. Companies are missing the point when they deal with each regulation as a single discrete effort that needs to be complied with. This myopic view of regulatory compliance creates the situation where organizations are constantly reinventing the wheel, wasting time and effort, and ultimately blowing security budgets.

The following white paper will detail a strategy that enables companies to painlessly gain PCI compliance and ensure effective security. By mapping technical controls to PCI standards and by continuously monitoring, assessing and reporting the status of your environment, Lumension's Security Suite will make your PCI audit the most efficient and actionable of your life.

The PCI Audit

PCI is elegantly simply in its implementation. A PCI audit consists of both on-site and off-site activities by a qualified security assessor (QSA). The audit team will evaluate an entity's payment and credit card security implementation against the PCI DSS standard.

The size of the PCI audit team is dependent on the size of an organization. It can be from a single QSA, all the way up to numerous auditors and a project manager.

A PCI engagement is generally performed in stages:

1. Assessment against the PCI DSS. Looking at items such as:
 - Policies and procedures; depth and breadth required
 - Key network design considerations for minimizing scope of an assessment
 - Key software development and application development functionality



- Scope of network devices, servers and workstations that are subject to PCI according to client's current infrastructure design
 - Action to be taken for each of the devices, servers and workstations in scope
 - Cost-effective methods for implementation and/or remediation that will meet compliance requirements
 - Prioritizing remediation efforts based on those items that may require the most time or become most pertinent prior to an on-site assessment
 - Acceptable incident response capability and/or improving upon [client possessive] existing capabilities in order to better meet requirements
2. Out-of-compliance (OOC) reporting
 3. Audit statement submission Report on Compliance (ROC).

While the items above are far from rocket science; if your staff is unprepared for the audit, it will be a painful experience. Besides being a waste of time, money and resources, the embarrassment of failing an audit due to lack of preparation clearly won't endear you to executive management.

Using a Framework for Security

The Fortune 1000 doesn't have a lack of information security products. Enterprise data centers are stocked full of racks of firewalls, VPN's, security appliances and much more. While the underlying infrastructure is there, the challenge enterprises face is making them work together, to provide adequate security, and to support the myriad regulatory and compliance requirements.

The bottom line is that the most effective and pragmatic method in which to deal with regulations is by creating an effective information security foundation and infrastructure. By creating this security foundation, an organization can easily deal with any new regulation that comes into law.

This is especially true given the compliance 80/20 rule. If you take all of the security and privacy regulations and combine them, there is roughly an 80% commonality between them. The 80/20 rule shows that having a core framework in place to deal with the 80% commonality means that at worst an enterprise will only have 20% of the new regulation to deal with.

That is where information security frameworks come into the picture. An information security framework contains the assumptions, concepts, risk values, and security practices underlying an organization's information security infrastructure. Frameworks such as ISO 27001¹ and 27002² and ITIL³ (IT Infrastructure Library) are needed because today's enterprise security

¹ ISO/IEC 27001 is the formal standard against which organizations may seek independent certification of their Information Security Management Systems (meaning their frameworks to design, implement, manage, maintain and enforce information security processes and controls systematically and consistently throughout the organizations).



projects are much more complex than those of years past.

SCAP

Perhaps one of the newest and most compelling frameworks is the Security Content Automation Protocol (SCAP). The primary intention of SCAP is to improve the application, verification, and reporting of security configuration settings.

The advantage SCAP has is that each vulnerability item is identified *once*. This common scheme prevents multiple entries for a single vulnerability. It is identified in one place where it is easily found. This enables everyone to work from the same vulnerability data set. By combining several standards enumerating security vulnerabilities and taking advantage of the combination, all of the critical information can be found in one place.

SCAP also seeks to encourage the development of automated checklists, particularly those that are compliant or compatible with the Extensible Configuration Checklist Description Format (XCCDF) and the Open Vulnerability and Assessment Language (OVAL). These are widely used for automated checklists - XCCDF primarily for mapping policies and other sets of requirements to high-level technical checks, and OVAL primarily for mapping high-level technical checks to the low-level details of executing those checks.

For example, XCCDF could map a requirement for authentication management in [NIST Special Publication 800-53](#) to a specified need to check that the system's minimum password length is at least 8 characters. OVAL could then define how that check should be performed on a particular type of system, such as a Vista or Linux based workstation.

Some of the benefits that SCAP affords include:

- The standardization of which security vulnerability and configuration information is identified and cataloged
- Ensuring that assessments are performed consistently (e.g., equal coverage, high quality, minimizing false positives/negatives, proper scan disposition)
- Supporting the traceability of specific security settings to corresponding compliance requirements
- Providing standardized scan criteria

Lumension has adopted this SCAP framework allowing organizations to leverage the power and flexibility of configuration checklists and technical controls and ultimately ensuring their security configurations are compliant with PCI standards.

² ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS).

³ ITIL is a customizable framework of best practices designed to promote quality computing services in the information technology sector



Pre-assessment Analysis

One of the biggest mistakes organizations make is to jump into the PCI remediation waters without first understanding what their gaps are. Every organization has a different maturity level when it comes to technology and compliance and it is important to know your level. Avoid the temptation to take a one size fits all approach to fixing your PCI gaps as such an approach will be costly in the long run, and it is unlikely that it will help you gain compliance in the short-term.

A pragmatic way to initiate your PCI compliance effort is via a pre-compliance assessment. This helps you understand where you are *today* with respect to PCI, in order to gain compliance *tomorrow*. Some of the items covered in the pre-compliance assessment include:

Item	Details
Infrastructure Review	Review of the IT infrastructure, PCI relevant application architecture, policies, procedures and processes, overall network design.
Gap Analysis	The gap analysis consists of defining the present state in reference to PCI compliance and the target state. Once this gap is identified, look at ways to bridge the gap defined.
Network Vulnerability Scanning	Lumension's Vulnerability Management solution, which integrates network discovery and vulnerability assessment, agent-based patch and remediation, and security configuration management, enables organizations to scan their environment for sources of risk and reports against PCI policy.
Risk Analysis	Not all risks are created equal. PCI requires you to understand the bigger pictures and then determine how to mitigate those risks.

The easiest and cheapest way to determine your current PCI state is by completing the PCI *Self-Assessment Questionnaire* (SAQ) from the PCI Security Standards Council. The PCI SAQ⁴ is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS. New in 2008 is that there are multiple versions of the PCI DSS SAQ to meet various scenarios.

The SAQ consists of questions correlating to the PCI DSS requirements, appropriate to service providers and merchants: The *Attestation of Compliance* is the certification that an entity is eligible to perform and has performed the appropriate Self-Assessment.

⁴ <https://www.pcisecuritystandards.org/tech/saq.htm>



Reducing PCI Scope

Reducing the scope of a PCI assessment is a great way to ensure that the effort is shorter and less costly. If yours is a flat network, with little or no separation between PCI and non-PCI systems, then PCI will apply to all of the systems within this environment. This shows that good network design is not only good for network efficiency, but can also lower the cost of your PCI compliance effort.

But if you can redesign the network and move PCI systems into their own dedicated environment and limit their interaction with non-PCI devices; this can significantly help reduce the number of critical systems to be in the scope of PCI. This in turn makes compliance cheaper and more expeditious. Consider routing and VLAN configurations that restrict access between the PCI networks.

Better Luck Next Time

Let's face it; unless you are one of the few organizations that took information security seriously from the get go, odds are that you will fail your PCI audit. There is nothing wrong with that as it is a near impossibility to go from non-compliance to PCI compliant in a few months.

With that, what you have to do is start planning for the next audit. The key is to see the areas in which you failed, and integrate those areas into your framework for compliance. There is nothing like an audit failure to get management interested. Use their short-term interest as a catalyst for moving PCI forward.

Get Management Commitment

While you have management's interest, it's important to realize that the ultimate success around PCI depends on how committed management is to it. If management cares, your organization is likely to have had effective security in the first place and it's likely you can achieve PCI compliance in the short term. If management doesn't care or is clueless, your organization's security is likely already in the hole and PCI failure is inevitable.

Organizations that have had the most success in their PCI efforts have done so by approaching PCI from a risk-driven model. Such an approach enables resources to be prioritized around business risks. This ensures that resources allocated are directly in line with those that contribute to the achievement of corporate objectives.

Such an approach is the cornerstone for an effective PCI compliance program management system. This is a formal system of risk management which can show that the PCI requirements and resulting work have been adequately planned and supervised. Notice that the operative word here is *formal*.

Lumension's Security Suite – A Way to Get You There

To optimally apply the investment made in your security and compliance programs,



Lumension's Security Suite delivers a powerful solution set that including Vulnerability Management, Endpoint Protection, Enterprise Data Protection and Compliance Management.

Vulnerability Management

Combining the crucial areas of PCI compliance with sound operational security practices, Lumension's Vulnerability Management Solution enables proactive discovery and assessment of IT assets, prioritization of threats, remediation of software and configuration vulnerabilities, including the customization of content, and advanced reporting capabilities. Delivering the only Vulnerability Management Solution that fully integrates network scanning and agent based assessment and remediation in a single management console, Lumension enables businesses to detect risks, deploy patches and defend their business information across a distributed environment with greater efficiency and with no impact to productivity.

Endpoint Protection

Lumension's Endpoint Protection Solution defends against all unauthorized and malicious software without relying on signature updates. Through central management of a trusted "whitelist" that defines a trusted application environment, Lumension Security Endpoint Protection protects against targeted and unknown attacks while enforcing the accepted IT policy. The result is a continuously enforced clean state that is malware and infection free, while also reducing IT support calls and promoting increased end user productivity.

Enterprise Data Protection

Lumension's Enterprise Data Protection Solution offers effective data security across endpoints and removable media with the most comprehensive enterprise-wide policy and granular control capabilities. By controlling and encrypting the flow of data onto removable devices and by providing robust forensics to quantify an organization's risk, Lumension ensures that sensitive business information is protected from loss or theft.

Compliance Management

Lumension's Compliance Management Solution provides a central repository for compliance data and compliance readiness that ensures continuous audit-readiness, actionable out-of-the-box and customizable reporting, regulatory compliance and corporate governance.

Lumension Security Suite

To address the many PCI DSS requirements, and the multifaceted requirements for security management, policies, procedures, network architecture, software design and other critical protective measures; Lumension's Security Suite enables the ingestion of the PCI policy template and maps technical controls to the detailed requirements. Lumension then automates the policy assessment of specific PCI requirements and monitors and reports against the requirements to ensure comprehensive PCI compliance.

Lumension's Security Suite proactively reduces business risk by ensuring systems are configured properly and delivers many compelling capabilities to ensure PCI compliance:

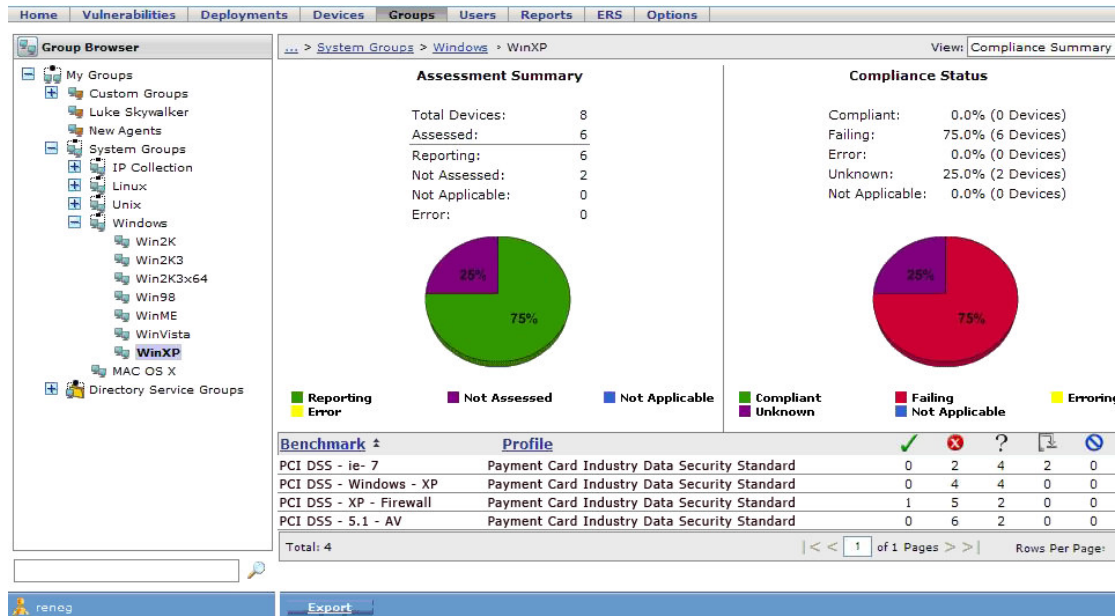
- Provides automated and continuous assessment, monitoring and comprehensive reporting
- Reduces corporate risk through the proactive assessment of configuration vulnerabilities



The Best PCI Audit of Your Life: Are You Ready?

- Employs best practice policy content such as the National Institute of Standards and technologies (NIST) National Vulnerability Database
- Embraces Open Standards for flexibility and wider capabilities including organization's own policies

The screen shot below shows the powerful Security Configuration Dashboard, which quickly gives you a comprehensive overview of the current PCI state. This particular screen shot shows a configuration summary view.



While the 12 PCI requirements are fundamental aspects of information security, the reality is that far too many organizations have not done their due diligence. It is that reason that they find the PCI requirements so onerous. The beauty of Lumension's Security Suite is that it can eliminate the arduous nature of PCI compliance efforts and enables you to focus on your business, all the while ensuring that you are audit-ready. The following table shows how Lumension's content maps to PCI DSS:

PCI Requirement	Specifics	Security Configuration Management
Protect Cardholder Data	<ol style="list-style-type: none"> 1. Install and maintain a firewall 2. Do not use vendor-supplied defaults 	Firewall Settings Local Policies Group System Settings
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data 	Network Settings System Settings Application Settings
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 5. Regularly update anti-virus software 6. Develop and maintain 	Security Patches Application Settings Network Settings



	secure systems	System Settings
Build and Maintain a Secure Network	7. Restrict access to cardholder data 8. Assign a unique ID to access computers 9. Restrict physical access	Local User Policy Settings Local Policies Group
Regularly Monitor and Test Networks	10. Monitor all access to network resources and cardholder data 11. Regularly test security systems and processes	Event Log Policy Settings Vulnerability Assessment
Maintain an Information Security Policy	12. Maintain a policy that addresses information security	XML – Prose in SCM template

Conclusion

Many think that PCI and costly assessments are synonymous. Lumension's Security Suite can indeed ensure that your PCI remediation effort is quicker, easier and cheaper.

Lumension's Security Suite is a powerful solution set that provides vulnerability management, endpoint protection, enterprise data protection and compliance management and reporting. By using Lumension's Security Suite in conjunction with the best practices approach described in this white paper, you can ensure that your PCI efforts can be done once and for all, and not in a haphazard manner. In fact, it may just turn into the best PCI audit of your life.

About the Author

Ben Rothke CISSP, CISM, PCI QSA (brothke@gmail.com) is a New York based Security Consultant and the author of *Computer Security: 20 Things Every Employee Should Know* (McGraw-Hill, 2006).