

Reducing the Cost of Achieving PCI Compliance with
Lumension Compliance and IT Risk Management

What Is It?

The [Payment Card Industry Data Security Standard \(PCI DSS\)](#) is a broad set of requirements developed to foster global adoption of consistent data security measures for any organization that processes, transmits or stores card member information. This specification encompasses security management, policy, procedure, network architecture, software design and other measures to ensure the security of customer payment information.

The standard has been developed and revised by the PCI Security Standards Council (PCI SSC), which is lead by a consortium of the five major payment brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.) with broader contributions from payment industry participating organizations. Adherence to the standard requires specific compliance certification by PCI SSC-sanctioned Approved Scanning Vendors (ASVs), which provide periodic vulnerability scanning of Internet-facing systems, as well as Qualified Security Assessors (QSAs), which validate adherence to the PCI DSS to provide confidence that cardholder information is adequately protected.

Who Has To Comply?

The swath of PCI DSS applicability is incredibly broad, as the number of global merchants relying on major credit card payments is staggering. PCI regulations apply more generally to those organizations that store, transmit or process cardholder information payments. This encompasses service providers, merchant acquirers, third-party processors and even data storage entities.

Processors represent organizations of significant transaction volume, which makes them tantalizing targets for attack. The breaches in late 2008 and early 2009 of RBS WorldPay and Heartland Payment Systems, which compromised more than an estimated 100 million cardholders, exemplify the irresistible allure of hackers to transaction processors.

What Are the Standards?

The PCI DSS foundation consists of 12 fundamental requirements organized into six major functional areas:

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 cardholder data

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

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder 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 for employees and contractors

The Challenges of Demonstrating Compliance

Organizations across the globe are required to demonstrate PCI compliance to ensure that cardholder data is protected and secure from numerous internal and external threats. The scope of demonstrating PCI compliance and passing an audit is determined by the number of credit card transactions handled each year and varies from company to company. Some organizations can get by with submitting a simple self-evaluation once a year while others are required to perform extensive audits more frequently and in greater depth.

The challenge for most organizations is that demonstrating compliance is usually performed on an ad hoc basis and without a clear process to regularly support multiple audit requests. Most organizations struggle to gather audit data and compliance measurements due to a lack of automated compliance workflows across the organization. Some of the typical issues around compliance include the following:

» Organizations Spend Too Much on Compliance

Many organizations often spend more on compliance than necessary. Inefficient and

costly compliance efforts are due to manual and disjointed IT audit processes. As regulatory requirements grow, organizations are increasingly turning toward the use of expensive third-party resources to help determine the impact of these requirements to their organizational policy. Compliance overspend also occurs when companies purchase multiple products to address each regulatory initiative separately.

» Organizations Lack Standardized IT Audit Processes

Most organizations do not know the status of their compliance and IT risk posture. Without a centralized data gathering approach to compliance reporting and audit workflows, organizations have a tough time demonstrating compliance with PCI or any other requirements. The reliance upon spreadsheets typically results in inaccurate reporting and ad hoc audits to locate information across multiple functional silos. Surveys to gather information on procedural and physical controls are typically conducted manually, resulting in disparate data collection and limited visibility into the organization's current compliance and IT risk posture.

Companies do not have a complete picture of IT risk across all their IT assets, and the current technology they are using only provides information on a section of a particular regulation. Lacking a comprehensive view of pertinent regulatory requirements and with IT assets scattered across multiple locations, organizations lack visibility into their compliance and IT risk posture.

» **IT Staff Must Provide Reports for Multiple Regulations**

Typically, a company must simultaneously comply with multiple regulations (for example, PCI and HIPAA), thus redundant processes and reporting occur:

- Companies purchase multiple compliance products, each to address a different and specific regulation or mandate.
- Multiple-point products produce disparate data that cannot be aligned to an organization's current compliance and IT risk posture.
- IT resources are repeatedly taxed to produce ad hoc reports for multiple compliance regulations, thus burdening already limited IT bandwidth.

» **Lack of Visibility and Prioritization of IT Risk**

Most companies have very limited capabilities when it comes to assessing IT risk and measuring PCI compliance. Because so much

valuable information is stored on corporate servers and workstations, it is vital for companies to get a better overall risk picture of their IT assets so they can prioritize resources against the assets that need their immediate attention.

Furthermore, most enterprises focus on IP-addressable assets but often exclude other numerous relevant resource types (e.g., databases, applications, user roles). This leads to limited visibility into all their business processes and their associated assets as well as their physical location.

Moving compliance initiatives from an ad hoc state to a standardized state is not only smart security, it's smart business. A standardized process ensures an efficient approach to demonstrating PCI compliance. With this approach you can establish your own framework to support PCI as well as other regulations, and correlate IT risk to your business.

PCI Compliance: Your Most Likely Audit

Of all the compliance regulations, mandates and guidelines, you're most likely to encounter PCI. Any vendor, organization, entity, group, business, etc., that accepts and processes credit cards falls under the PCI requirements standard and is subject to its audit cycles. PCI DSS covers a range of physical and technical controls that must be measured and reported on through network scans and surveys. Some PCI compliance mandates lend themselves well to electronic scans for evidence of controls. Other physical and procedural controls for PCI must be evaluated through surveys that are sent to respective owners for verification.

Looking more closely at the PCI DSS standard reveals a number of specific areas that must be addressed by any organization that must achieve PCI compliance. The areas include:

» Data Protection

The foundation of the DSS standard is protection of payment cardholders' data. The financial implications of breaches at a processor or large merchant have the potential to impact hundreds of thousands, or in some cases even millions, of cardholders' financial lives.

A recent study highlights the increasing number of data exposures, as reports of data breaches in the United States increased 47 percent in 2008 compared with the previous year.¹ It is critical that merchants and processors protect against all types of data leakage from novel and established, external and internal threats.

» Vulnerability Management

PCI DSS emphasizes vulnerability management as one of the six areas that must be addressed by merchants, underscoring its importance in achieving data security. An organization must look at vulnerability management from the perspectives of people, processes and technology to be effective. Many solutions in the vulnerability management and compliance space do not encompass the full management cycle with some solutions focusing only on a single area such as assessment or reporting. A complete vulnerability management solution should be able to Discover, Assess & Prioritize, Define & Implement Policies, Remediate & Enforce as well as Monitor & Report.

» Effective Anti-Malware

The widely published breach of Heartland in January 2009, which utilized data-sniffing malware on the payment processors' servers, illustrates the constant evolution of attack vectors. This continued critical conversation regarding the PCI DSS standard itself. This criticism has covered the scope of the regulation, including the difficulties of achieving compliance, the need for more situational adaptability and risk-based orientation, and the ineffectiveness of the PCI's controls. The individual payment card brands vigorously defend the standard, noting, "no compromised entity has yet been found to be in compliance with PCI DSS at the time of a breach."²

¹ "Ten Common Myths of PCI DSS by PCI SSC LLC

² Ellen Richey, Visa's Chief Enterprise Risk Officer in

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130073>

How Lumension Compliance and IT Risk Management Helps Achieve PCI Compliance

Lumension solutions can measure levels of PCI compliance, deliver data protection and realize full-cycle vulnerability management.

[Lumension® Compliance and IT Risk Management](#) addresses PCI DSS by providing the key capabilities to Identify, Assess, Remediate and Manage your network to demonstrate PCI compliance on a regular basis.

A primary component of this solution is provided by [Lumension® Risk Manager](#), a powerful solution that allows organizations to immediately improve their IT audit workflow and then assess their IT risk posture against internal and external regulations such as PCI. As a result, customers can reduce their overall cost of compliance by streamlining the IT audit process, unifying control and compliance frameworks, automating assessment and remediation processes, and enabling continuous monitoring of their compliance and IT risk management posture.

Key features of Lumension Compliance and IT Risk Management allow you to standardize your compliance approach and include:

- » Risk Profiling: Model relationships between your IT assets and business interests to identify areas of business risk. Lumension Risk Manager categorizes an organization's resource types, including people, processes and technology, to develop a powerful risk profile through its

patent-pending risk intelligence engine. The risk profile information is automatically correlated with internal and external compliance requirements to mitigate IT controls and address potential regulatory and IT risk exposure.

- » Controls-Based Framework: Leveraging the industry-standard [Unified Compliance Framework \(UCF\)](#), Lumension Risk Manager harmonizes controls across hundreds of different regulations and control frameworks, including PCI, SOX, FISMA, [HIPAA](#), [NERC](#), COBIT, NIST, ISO27001 and many more. This means that no control is ever duplicated and the structure and language of each control follow the same predictable format.
- » Controls Assessment: Lumension Risk Manager streamlines and automates your workflows for assessing technical, physical and procedural controls for PCI by interfacing with either Lumension security solutions or third-party vulnerability scanners. Plus, it utilizes automated surveys to complete your assessment of physical and procedural controls.
- » Risk & Compliance Reporting: Generate reports with key metrics to satisfy a diverse IT risk and compliance audience through compliance and IT risk reporting, operational security reporting and remediation modeling and forecasting. Lumension Risk Manager creates "what-if" scenarios to better estimate how a project or remediation effort will improve your IT risk and compliance posture.

Lumension's operational endpoint management and security solutions further address PCI compliance by enforcing security policies. These capabilities include:

» **Incorporation of Scan Data for PCI**

Compliance: Extensive, cross-referenced [vulnerability assessment](#) metadata providing a complete and prioritized view of security exposures.

» **Remediation to Help Achieve PCI**

Compliance: The capability to create custom remediation packages to address configuration, software and service removal, and patching for internally developed applications.

- Continuously updated [software patch](#) subscription feed for use by the remediation engine

» **Application and Device Controls to Help Achieve PCI Compliance:**

- Server lockdown enabling only [whitelisted applications](#) and preventing the execution of malicious code
- Removable device protection integrating [enforcement of encryption](#) and [device control](#) policy while accommodating granular administrative rights control

The following table illustrates the depth of Lumension's solutions and how they work together to identify, assess, remediate and manage your network to achieve PCI compliance and greater levels of overall network security.

Compliance Standards	Lumension Solution	How Lumension Helps
All PCI Requirements	Lumension Compliance and IT Risk Management	Lumension® Risk Manager allows organizations to immediately improve their audit workflow and then assess their IT risk posture against internal and external regulations. Customers can reduce their overall cost of PCI compliance by streamlining the IT audit process, unifying control and compliance frameworks, automating assessment and remediation processes, and enabling continuous monitoring of their compliance and IT risk management posture.
Requirement 1 (R1): Install and maintain a firewall configuration to protect data	Lumension® Vulnerability Management	Lumension® Content Wizard can automate the installation or removal of any software packages across heterogeneous platforms. Leveraging this functionality to deploy personal firewall software on remote machines would help an organization achieve compliance with R1. Lumension® Scan provides complete asset discovery and inventory, which can help identify and document services in use that are bound to specific network ports to help comply with the services, ports and protocols documentation element of R1.

Compliance Standards	Lumension Solution	How Lumension Helps
<p>Requirement 2 (R2):</p> <p>Do not use vendor-supplied defaults for system passwords and other security parameters</p>	<p>Lumension® Vulnerability Management</p>	<p>By utilizing Lumension Scan’s flexible credentials management capability, multiple computing systems can be tested to verify that vendor-supplied defaults have been changed per R2.</p> <p>Lumension® Security Configuration Management assesses configurations utilizing NIST-established, SCAP- based standards consistent with the PCI R2 DSS’s testing guidance to “verify the system configuration standards are consistent with industry-accepted hardening standards.”</p> <p>Lumension Content Wizard provides IT management with a framework to develop and deploy configuration control extending to protocol/port restriction through scripted configuration delivery as needed to comply with R2. This same approach can be utilized to configure system parameters to prevent misuse and remove unnecessary functionality.</p>
	<p><u>Lumension® Endpoint Protection</u></p>	<p>R2 specifies disabling all unnecessary and insecure services and protocols. Lumension® Application Control is ideally suited to the task of ensuring that unnecessary or undesired services are not active through its application lockdown capability.</p>
<p>Requirement 3 (R3):</p> <p>Protect stored cardholder data</p>	<p><u>Lumension® Data Protection</u></p>	<p>Lumension® Device Control enforces encryption policies for portable digital media, helping ensure compliance with R3 to render the PAN unreadable.</p>
<p>Requirement 4 (R4):</p> <p>Encrypt transmission of cardholder data across open, public networks</p>	<p>Lumension Vulnerability Management</p> <p>Lumension Compliance and IT Risk Management</p>	<p>Though Lumension’s products are not utilized directly for encryption of the transmission of cardholder data over public networks, Lumension Vulnerability Management can aid a processor in demonstrating compliance and verify that the latest patched versions of encryption packages such as SSH or TLS are in place per R4.</p> <p>Lumension Compliance and IT Risk Management can assist the organization in documenting internally or for the QSA such patch status across the servers in the organization.</p>

Compliance Standards	Lumension Solution	How Lumension Helps
<p>Requirement 5 (R5):</p> <p>Use and regularly update anti-virus software or programs</p>	<p>Lumension Endpoint Protection</p>	<p>PCI's compliance assessment includes the use of compensating controls, which may be utilized when "due to legitimate technical or documented business constraints" the organization cannot explicitly meet the PCI DSS requirement as stated.³ Lumension Endpoint Protection provides automated application discovery and application whitelisting, which can be utilized to provide server lockdown, preventing the execution of malicious code on Windows systems. This application whitelisting approach may be seen as an alternative control to address the anti-virus requirements to "deploy anti-virus software on all systems commonly affected by malicious software" and to "ensure that all anti-virus mechanisms are current, actively running and capable of generating audit logs."</p>
<p>Requirement 6 (R6):</p> <p>Develop and maintain secure systems and applications</p>	<p>Lumension Vulnerability Management</p> <p>Lumension Compliance and IT Risk Management</p>	<p>Lumension Vulnerability Management is a lynchpin for a merchant or processor to achieve compliance with the multiple facets of R6. Lumension Vulnerability Management enables an organization to maintain a rigorous vulnerability management lifecycle program from vulnerability assessment to remediation to compliance. Comprehensive and actionable reporting is available through Lumension Compliance and IT Risk Management.</p> <p>Lumension Vulnerability Management delivers subscription-based updates providing the transaction processor merchant with the latest vulnerability information to secure and protect its transaction-processing environment. Valuable metadata (e.g., cross-referencing CVE to MSRC numbers) concerning vulnerabilities is provided to administrative personnel to ensure the most complete perspective of emerging vulnerabilities detected on their systems and to initiate the most appropriate and effective response.</p> <p>Lumension Vulnerability Management can help any enterprise ensure all applications that are developed or implemented in-house follow a secure software development methodology. Lumension Vulnerability Management also enables remediation of not only standard applications across heterogeneous OSs but also enables patching of the OSs themselves. Additionally, Lumension Content Wizard enables the rapid creation of custom remediation packages to facilitate securing specialized applications developed in-house or by third-party software vendors.</p>

³A compensating control must be thoroughly evaluated by a QSA to validate that it adequately addresses the risk of the original DSS requirement

Compliance Standards	Lumension Solution	How Lumension Helps
<p>Requirement 7 (R7):</p> <p>Restrict access to cardholder data by business need to know</p>	<p>Lumension Data Protection</p>	<p>Lumension Data Protection restricts data-in-motion by per-user permissions and enables “need to know”-based access control solutions. Lumension’s solution is well-suited to the PCI requirements providing a Whitelist/“Default Deny” configuration that requires specific device access be enabled and helps enterprises provide complete privilege-based access control solutions.</p> <p>The requirement to limit system component access to only required individuals is aided by Lumension Data Protection, which can restrict Windows device access and utilizes per-device permissions to control numerous data pathways and to uniquely identify/authorize specific media.</p> <p>Lumension Device Control’s centralized administration, which provides flexible policy with granular control, further accommodates privileged assignment based on job classification.</p>
<p>Requirement 10 (R10):</p> <p>Track and monitor all access to network resources and cardholder data</p>	<p>Lumension Data Protection</p>	<p>Lumension Data Protection provides logging capabilities that can enable an enterprise to achieve compliance with user-based system component access tracking.</p> <p>Lumension’s powerful logging and reporting provides full compliance with R10. Syslog messages address all the sub-requirements by providing timestamp, user, message code and severity, device type and name, and machine name.</p> <p>R10 also requires backing up audit trails to a centralized log server or media that is difficult to alter. This could be accommodated by Lumension Data Protection’s capability to enforce encryption for removable storage, including write-once optical media.</p>
<p>Requirement 11 (R11):</p> <p>Regularly test security systems and processes</p>	<p>Lumension Vulnerability Management</p>	<p>Lumension Vulnerability Management allows merchants or service providers to conduct non-intrusive production-ready scans via agent- and network-based mechanisms. The use of credential-based scans provides highly accurate vulnerability cross-reference maps that provide an enterprise with maximum visibility into its vulnerability exposures. Lumension’s scanning solution can help an enterprise comply with its internal and external scanning requirements after a network change.⁴</p>

⁴Quarterly external vulnerability scans must be performed by an ASV qualified by PCI SSC.

Financial Implications

The financial penalties for non-compliance are associated with the legal agreements that a merchant or processor has with the individual payment card brand (or processor). Such payment brand program compliance penalties exist for non-compliance at the time of the incident as well as failure of the merchant or service provider to notify the brand of the data breach. Penalty limits of up to \$500,000

for payment brand program non-compliance at the time of the breach and \$100,000 for failure to notify are not unusual for an individual payment brand.

In addition, the potential loss to the merchant/processor from losing the ability to process a specific payment brand (or utilize a processor) brings financial implications that may threaten the livelihood of the business itself.

Specific MasterCard Financial Penalties:

Non-compliance Category	Assessment Type	Assessment Description
Category A Payment System Integrity	Per Violation	First Violation: Up to \$25,000
		Second Violation within 12 months: Up to \$50,000
		Third Violation within 12 months: Up to \$75,000
		Fourth and Subsequent Violations within 12 months: Up to \$100,000 per violation
Category B Visible to Customers	Per Violation	First Violation: Up to \$20,000
		Second Violation within 12 months: Up to \$30,000
		Third Violation within 12 months: Up to \$60,000
		Fourth and Subsequent Violations within 12 months: Up to \$100,000 per violation
Category C Efficiency and Operational Performance	Per Violation	First Violation: Up to \$15,000
		Second Violation within 12 months: Up to \$25,000
		Third Violation within 12 months: Up to \$50,000
		Fourth and Subsequent Violations within 12 months: Up to \$75,000 per violation

http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf

Conclusion

Moving from an ad-hoc to a standardized approach to PCI compliance is possible with the right solution. To achieve a state of continuous compliance and reporting, it is necessary to deploy solutions that can Identify, Assess, Remediate and Manage all compliance initiatives across the network. Using Lumension's Compliance and IT Risk Management solution allows enterprises to:

- » Identify network assets, including servers, databases, applications, etc.
- » Assess levels of compliance for all regulations, including PCI
- » Remediate identified vulnerabilities and prioritize IT risk
- » Manage compliance reports and provide real-time PCI reports whenever required

In today's challenging economic and regulatory environment, it's time for organizations to move away from "clipboard" compliance and streamline audit processes to reduce your cost of PCI compliance.

About Lumension

Lumension, a global leader in operational endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-

winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Compliance and IT Risk Management offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year.

Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, India, Hong Kong and Singapore. Lumension: IT Secured. Success Optimized. More information can be found at www.preventia.co.uk



Additional Research

Video: Success Story

[EC Suite meets PCI compliance requirements with proactive endpoint security solution](#)

[Whitepaper: Five Ways to Reduce Your Audit Tax](#)

[Aberdeen Group Report – IT GRC: Managing Risk, Improving Visibility and Reducing Operating Costs](#)

Key Steps to Ensuring PCI Compliance

[Watch the Demo: Addressing PCI DSS Compliance with Lumension® Risk Manager](#)

[Request a Personal Demonstration of Lumension Risk Manager](#)