

# Best Practice Guide to Reducing Your Cost of Compliance

## Executive Summary

With IT budgets barely keeping up with inflation in 2012 and the cost of compliance expected to rise, organizations must find ways to streamline compliance spending to maintain IT operations and IT security service levels in the coming year. Here are some useful best practices to slash regulatory overhead and improve the effectiveness of your compliance spend.

### Overview

No matter how you look at it, compliance isn't cheap. As IT groups grapple with the cascade of new regulations, security standards, laws and mandates that seem to come out almost monthly, they're placed in a seemingly impossible situation. Governing bodies offer little flexibility in compliance, which continues to increase the cost of IT security moderately to significantly for most organizations. At the same time, many IT groups are still asked by business executives to maintain flat or even declining budgets to adjust to economic pressures while meeting compliance objectives.

The very smartest organizations understand that even though compliance spending is a must in the modern budget, those dollars needn't come at the

expense of other critical IT spending priorities. By following several common sense best practices and employing the right automated tools, best-in-class organizations are able to reduce compliance overhead and maximize the dollars they do spend in such a way that they not only fulfill compliance demands but also offer meaningful security improvements.

### Which Data Protection Regulations Must You Comply With?

There are multiple data protection rules and regulations with overlapping jurisdictions, including pan-national (e.g., the EU), national, state and even non-governmental or industry-specific rules. Further resources to assist you in understanding all the compliance requirements to which you be subject can be found in [Appendix A](#); this includes:

[United States](#)

[United Kingdom](#)

[European Union](#)

[Asia and the Pacific Islands](#)

[Additional Jurisdictions](#)

[Non-Governmental](#)

[Critical Infrastructure Protection Requirements](#)



### The Hidden Cost of Spreadsheets

If you are currently using spreadsheets or databases to manage business critical activities like risk and compliance, then you'll know that they have some big disadvantages. Not only are spreadsheets and databases hard to maintain and audit, they also lack visibility and accessibility to the key stakeholders across the organization. Click here to learn more about the [Hidden Cost of Risk Management by Spreadsheet](#).



Continued »

### How Compliance Costs Organizations

- » **Money:** PCI compliance costs an average of \$2.1 million among Level 1 merchants and \$1.1 million among Level 2 – 4 merchants.<sup>1</sup>
- » **Time:** 71 percent of organizations believe they'll need to spend more time liaising with regulatory bodies in 2012.<sup>2</sup>
- » **Complications:** Some IT groups that rely on manual tracking processes have to juggle as many as 40,000 different spreadsheets to demonstrate compliance.<sup>3</sup>

### How to Reduce the Compliance Burden

Compliance continues to hog the bandwidth of business and IT executives alike, scoring as one of the top security priorities of large organizations in 2012. But even as the majority of organizations are upping their fiscal outlay to comply with security regulations, many fail to take advantage of that spend to make lasting security improvements. For example, surveys have shown that only 36 percent of organizations have actually implemented continuous monitoring of security controls. And only 11 percent of organizations report that their IT security improved in 2009 due to increased regulations. Streamlining compliance procedures, automating reporting and improving visibility into controls makes it possible to allocate more dollars to other IT operations security projects. And better syncing security practices and metrics into compliance efforts ensures that the remaining money returns the best security dividends.

1. Gartner, [PCI Compliance Activity Shifts Downstream as Aggressive Enforcement Continues](#), June 2008
2. Complinet, [Cost of Compliance Survey 2011](#), July 2011
3. Corporate Integrity, LLC, [Foundations of GRC: Streamlining Compliance](#), May 2009

Continued »

## Best Practices to Reduce the Compliance Burden

Best Practices	How Lumension Helps
<p><b>1. Streamline Gap Analysis:</b> Streamline gap analysis to quickly find requirement changes in updated regulations and additional requirements in new regulations that are currently unmet by existing IT security practices.</p>	<ul style="list-style-type: none"><li>• Uses Unified Compliance Framework (UCF) to review and update compliance requirements across hundreds of regulations, including PCI, SOX, FISMA, HIPAA, NERC and more.</li><li>• Allows you to stay current with changing regulations, and maintain a detailed record of your compliance posture with previous versions of regulatory requirements.</li><li>• Enables comparison of existing IT controls with new control requirements to offer recommended changes for improved compliance with regulations targeted by executive decision-makers.</li><li>• Control harmonization ensures no control is ever duplicated and the structure and language of each control follows the same predictable format.</li></ul>
<p><b>2. Kick Spreadsheets to the Curb:</b> Eliminate spreadsheets and automate the information-gathering process necessary to prove compliance with specific regulatory requirements.</p>	<ul style="list-style-type: none"><li>• Avoids redundancy and inconvenience to employees by requesting a single set of relevant survey questions from each business unit and automatically cross-referencing answers to multiple regulations.</li><li>• Prevents costly oversights in queries that arise through disorganized manual processes, reducing risk of expensive audit failures.</li><li>• Does away with time-consuming processes needed to track IT asset and survey information on spreadsheets, offering visibility into controls without excessively diverting IT and business unit employees from more important duties.</li></ul>

Continued »

Best Practices	How Lumension Helps
<p><b>3. Mesh Compliance and Security Practices:</b> Overlay security practices on top of compliance efforts to avoid “checkbox compliance” mentality and maximize real security effectiveness through required compliance spending.</p>	<ul style="list-style-type: none"><li>• Interfaces with Lumension security solutions or third-party point products such as vulnerability scanners to assess technical controls.</li><li>• Models the relationship between IT assets and business interests to identify IT-borne business risk.</li><li>• Leverages a patent-pending risk intelligence engine that uses the risk profile of each asset to automatically identify the controls it needs to achieve compliance and mitigate risk.</li><li>• Maps existing security practices against IT security frameworks such as CoBIT, ISO and more to analyze for gaps in controls that can be targeted to reduce threat exposure and achieve compliance.</li></ul>
<p><b>4. Prepare for Consultants and Auditors:</b> Make the most of your outsourced consultants’ time by eliminating costly searches for compliance information and statistics.</p>	<ul style="list-style-type: none"><li>• Enables even small organizations to collect and organize relevant compliance information before a consultant or outside auditor arrives.</li><li>• Prompts organizations for missing information that consultants will request.</li><li>• Offers the flexibility to either prepare information in ready-made reports or to grant consultants or auditors access to relevant information feeds tied to IT resources and already-completed surveys.</li></ul>

Continued »

Best Practices	How Lumension Helps
<p><b>5. Provide Executives with Business-Friendly Information:</b></p> <p>Give decision makers actionable information to improve budget prioritization and avoid the costly cleanup that comes after flagging an audit.</p>	<ul style="list-style-type: none"><li>• Provides total, automated visibility over the IT network and endpoint infrastructure to identify blind spots covered by regulations that may otherwise go overlooked during manual internal audits.</li><li>• Offers “what-if” simulations that allow IT leaders to enter variables based on proposed security purchases or mitigations that will return quantitative metrics, allowing IT leaders to communicate to decision-makers exactly how much more compliant a project will make the organization.</li><li>• Generates reports with compliance results and metrics in layman’s terms to better aid the IT-to-business unit translation process during board meetings and C-level briefings.</li></ul>

Continued »

### Key Lumension Solutions [Lumension® Compliance and IT Risk Management](#)

Provides a comprehensive view across hundreds of global regulations, mandates and internal policies, improving the efficiency of controls and reducing risk with the flexibility to easily accommodate evolving requirements and enable real-time visibility of the level of compliance achieved. Lumension enables visibility for compliance and IT risk through four key capabilities:

- » Risk Profiling
- » Controls Framework
- » Controls Assessment
- » Risk & Compliance Reporting

### Additional Resources

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

This whitepaper outlines five methods organizations should consider to streamline their compliance efforts and thereby reduce their audit tax.

#### [Webcast: Harmonizing Controls to Reduce Your Cost of Compliance](#)

This webcast examines the Unified Compliance Framework and how Lumension leverages it within its compliance and IT risk management solution to harmonize controls across hundreds of regulations. Learn how to eliminate overlapping control requirements and ensure a more efficient and less costly approach to compliance.

#### [Solution Demonstration: Lumension® Compliance and IT Risk Management](#)

Walk through a demonstration of Lumension® Compliance and IT Risk Management solution and learn how to identify optimal compliance controls; assess technical, physical and procedural controls; remediate compliance deficiencies based on your priorities; and manage your overall compliance effort with operational and strategic visibility and reporting.

#### [Resource Center: Reduce Your Cost of Compliance](#)

This resource center is designed to help your research efforts and contains whitepapers, videos, analyst research and product information to guide you through key strategies to streamline audit and IT risk management workflows and to cost effectively ensure continuous compliance.

### Appendix A Data Protection Regulations Around the World

There are multiple data protection rules and regulations with overlapping jurisdictions, including pan-national (e.g., the EU), national, state and even non-governmental or industry-specific rules. Below are a few rules and regulations, in addition to further resources to assist you in understanding compliance requirements.

#### United States

The U.S. has many data protection and privacy laws and regulations that affect different industries. Below are some of the most recognizable.

- » [Healthcare Industry](#): Examples include [HIPAA](#) and [HITECH](#)
- » [Financial Industry](#): Examples include [PCI DSS](#), Red Flag Rules, SOX and GLBA
- » [Federal Government](#): Examples include [FDCC](#), [FISMA](#) and [SCAP](#)

Currently, 49 states and territories have data breach notification laws. One of the most stringent of these laws is [MA 201 CMR 17](#), which went into effect in March 2010. It covers:

- » In-state and out-of-state companies with operations or customers in Massachusetts.
- » Every organization which owns, licenses, stores or maintains personal information about a resident of the Commonwealth.

[Visit the National Conference of State Legislatures \(NCSL\) online to learn more about data breach notification laws by state.](#)

#### United Kingdom

The Data Protection Act (DPA) covers any data that can be used to identify a living person, including names, birthday and anniversary dates, addresses, telephone numbers, fax numbers, e-mail addresses, etc. It only applies to that data which is held, or intended to be held, on computers (“equipment operating automatically in response to instructions given for that purpose”) or held in a “relevant filing system.”

[View the UK Data Protection Act.](#)

#### European Union

The European Commission has a website dedicated to the data protection legislation.

[Learn more about the EU data protection laws.](#)

#### Asia and the Pacific Islands

There is a wide range of legislation through Asia and the Pacific Islands regarding data protection.

[Learn more about the laws pertaining to these countries.](#)

### Additional Jurisdictions

A by no means exhaustive list includes:

- » Canada: [Personal Information Protection and Electronic Documents Act](#) (PIPEDA)
- » Mexico: [Ley Federal de Protección de Datos Personales en Posesión de los Particulares](#) (LFPDPPP)
- » *Habeas Data* laws in Latin American countries such as Argentina, Brazil, Paraguay and Peru
- » Australia: [Privacy Act 1988](#)
- » South Africa: [Protection of Personal Information Bill](#)

### Non-Governmental

Probably the most pervasive non-governmental data protection requirement is [the Payment Card Industry Data Security Standard](#) (PCI DSS), which covers all organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. This includes most organizations in the [retail](#), [financial](#), [healthcare](#), utility and even government sectors.

### Critical Infrastructure Protection Requirements

Another example of non-governmental information security requirements are the [Critical Infrastructure Protection \(CIP\) Cyber Security Standards](#) from the North American Electric Reliability Corporation (NERC), which is the Electric Reliability Organization (ERO) for Canada, the US and part of Baja California, Mexico. Commonly referred to as the [NERC CIP Standards 002-009](#), these cover everything from critical asset identification and management to physical and systems security to incident reporting and recovery planning.

### About Lumension Security, Inc.

Lumension Security, Inc., a global leader in 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, Antivirus and Reporting and Compliance 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 Texas, Florida, Washington D.C., Ireland, Luxembourg, Singapore, the United Kingdom, and Australia. Lumension: IT Secured. Success Optimized.™ More information can be found at [www.lumension.com](http://www.lumension.com).

Lumension, Lumension Compliance and IT Risk Management, “IT Secured. Success Optimized.”, and the Lumension logo are trademarks or registered trademarks of Lumension Security, Inc. All other trademarks are the property of their respective owners.



#### **Global Headquarters**

8660 East Hartford Drive, Suite 300  
Scottsdale, AZ 85255 USA  
phone: +1.480.970.1025  
fax: +1.480.970.6323

[www.lumension.com](http://www.lumension.com)

Vulnerability Management | Endpoint Protection | Data Protection | Compliance and IT Risk Management