

Measure Your Security Posture and Prioritize Your IT Risk

Many organizations face the challenge of continuously measuring IT risk, communicating IT risk with senior management and prioritizing security projects to address the risk that has the greatest business impact. Without the ability to consolidate numerous sources of IT risk information and correlate risk across all IT assets in a network, an organization cannot effectively measure the business impact and ensure continuous compliance with internal security policies or external mandates.

Streamline Controls Assessment and Demonstrate Compliance to Reduce IT Security Costs

By harmonizing controls across hundreds of regulations, frameworks and internal policies, security professionals can ensure there are no redundant survey efforts. Automating IT risk assessment workflows across technical, physical and procedural controls through the use of third party connectors and automated surveys can reduce audit preparation, cost and reporting of compliance and security posture.

Lumension® Risk Manager:

- » Continuously measures your IT security posture and gathers data to demonstrate compliance with internal policies and external regulations
- » Identifies and prioritizes potential IT risk by correlating IT assets (i.e. servers, workstations, applications, etc.) to critical business processes, compliance regulations and control frameworks
- » Automates the gathering of IT risk assessment data through integration with Lumension products and a wide range of third party tools (i.e. vulnerability scanners, etc.)
- » Benchmark risk assessments against IT control frameworks
- » Improves understanding and communication of security posture metrics to IT staff and senior management

Key Features

Risk Profiling and Security Posture: Models the relationship between IT assets and business interests to identify IT-borne business risk. Measures and reports on security posture.

- » **IT Asset Catalog with Comprehensive Resource Types:** Going beyond just IP-addressable assets, all resource types are included in the LRM database, such as applications, databases, servers, networks, data centers, people and processes.
- » **Patent-Pending Risk Intelligence Engine:** Correlates risk profile information with compliance requirements and automatically identifies mitigating IT controls to address any potential regulatory and IT risk exposure.
- » **Controls Framework:** Harmonizes controls across different regulations including PCI, SOX, HIPAA, COBIT, NIST and hundreds more.
- » **Unified Compliance Framework (UCF):** Lumension Risk Manager utilizes the industry-vetted and harmonized mapping of unique controls that spans more than 400 global compliance regulations and mandates. New modular content packs, including updated UCF content simplifies the upgrade process
- » **Scenario-based risk modeling and metrics:** Compare compliance activities side-by-side and use “what if” scenarios to determine how applying different resources will have the greatest benefit to your scores.

Key Benefits

- » Provides Continuous Measurement of Your Security Posture through dashboards and key metrics
- » Aligns and Prioritizes IT Risk to IT assets to measure and report on Business Impact
- » Streamlines IT Risk Assessment and Visibility to Better Demonstrate Compliance
- » Improves Visibility of IT Risk for Senior Management and Business Leaders through clear reports

“Lumension® Risk Manager has been an excellent investment for our IT security program. It has allowed us to maximize our IT security resources by prioritizing our efforts on areas that matter most to the business, and it allows us to manage what needs to be done and how to accomplish those tasks.”

Jonathan Steenland, CISSP,
Security Officer, Fujitsu America

Key Features Continued

Controls Assessment: Automated assessment of technical, physical and procedural controls.

- » **Streamlined Workflow for Assessing Physical and Procedural Controls:** Automated risk assessment workflow provides structure around the process of collecting risk scores and providing evidence for physical and procedural controls.
- » **Automated Self-Assessment Surveys:** Send multiple-choice surveys to system owners to request up-to-date control implementation status for their areas of responsibility. Once approved, survey responses automatically update risk scores.
- » **Interfaces with Security Point Solutions:** Connectors to Lumension security solutions and third party point products such as vulnerability scanners, with field-configurable connectivity via SQL and automated data import and processing of XML and flat-file data. These connectors collect operational security data from your network to automatically update risk scores and measure levels of compliance.
- » **Attachments for Evidence Collection:** Provides a convenient way to manage the myriad of evidence artifacts required to demonstrate the validity of self-assessment scores.
- » **Exception Management:** Provides flexibility to mark risk scores as “exempt” for a fixed period of time, with the exception state visible, but not counted in the compliance and IT risk calculations.
- » **Score Sync Plugin:** Allows a score to be automatically synchronized to multiple subjects whenever it’s updated and this control score can be inherited across different groups.

Risk & Compliance Reporting: Generate reports and metrics to satisfy a diverse IT risk and compliance audience.

- » **Custom Reports and Dashboard Views:** Integration of report links into in-product menus, improved custom report parameter entry panels, and the ability to publish/share custom dashboard views with other users.
- » **Compliance and IT Risk Reporting:** Compliance reports demonstrate degrees of compliance as they pertain to regulations or internal policies. IT risk reports catalog security gaps and how they could affect key business interests.
- » **Operational Security Reporting:** Provides detailed security gap and trending information across IT operations. Extensions to CDK (Connector Development Kit) enable detailed operational security reports on the systems LRM connects to. For example, produce a detailed patch status report directly from the LRM dashboard.
- » **Remediation Modeling and Forecasting:** Create “what-if” project scenarios to estimate how a project or remediation effort will improve your IT risk and compliance metrics.
- » **Remediation Tracking:** Provides assignment and status tracking of remediation projects with scores automatically updated to reflect improvement in compliance and IT risk metrics.
- » **E-mail Notifications:** Alerts, which are configurable to specific users/groups provide notifications of key conditions and state changes within compliance measurements.

www.lumension.com

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

System Requirements

- » **Server:** Windows Server 2003 / 2005 / 2008, SQL Server 2005/2008, SQL Server 2005 Express Edition

[Complete Requirements](#)

Online Resources

- » [Compliance and IT Risk Mgmt. Blog](#)
- » [Demystifying IT Risk to Achieve Greater Security and Compliance](#)
- » [Bottom Up vs. Top Down Approach to Compliance and IT Risk Management](#)
- » [Compliance or Security: What Comes First?](#)
- » [Five Ways to Reduce Your Audit Tax](#)
- » [PCI DSS Compliance and Security: Harmony or Discord?](#)

Contact Lumension

- » Global Headquarters
8660 E. Hartford Dr,
Suite 300
Scottsdale, AZ 85255
+1.480.970.1025
sales@lumension.com
- » United Kingdom
+44.0.1908.357.897
sales.uk@lumension.com
- » Europe
+352.265.364.11
sales-emea@lumension.com
- » Asia & Pacific
+65.6725.6415
sales-apac@lumension.com

