



## LMI is critical for solving the following complex business requirements:

- › Comply with multiple regulations and mandates.
- › Answer specific mandates related to log data.
- › Pass critical audits and provide a strategy to ensure ongoing compliance.
- › Reduce the cost and complexity of audit processes, such as sampling.
- › Eliminate secondary audit costs.
- › Automate production of reports, alerts and sampling.
- › Ensure data is preserved in an immutable form for litigation.
- › Confidently attest to data quality, IT controls and compliance.
- › Align business and IT initiatives.

GLOBAL MANDATES	
Regulations	Retention Requirement
PCI	1 Year
EU DR Directive	2 Years
NERC	3 Years
FISMA	3 Years
GLBA	6 Years
Basel II	6/7 Years
HIPAA	6/7 Years
SOX	7 Years

## LogLogic Compliance and Control Suites™

Increasingly, businesses are looking to Log Management and Intelligence (LMI) technologies to comply with regulations and industry mandates. In many instances, LMI is required specifically to comply, and in all cases managing logs is a critical activity for enforcing and attesting to IT controls, conducting investigations and producing audit samples. An LMI platform isn't just the best way to achieve continuous compliance, it's the first step in reducing cost and complexity and removing the burden of an ever increasing number of regulations, controls and audit requirements.

Log data can account for over 30% of all enterprise data, and strategies to make that data useful for compliance are being sought by the Global 2000, totaling almost \$1B in investments. LMI provides a fingerprint of user activity and log data generated by applications, services, and network devices is now, through LMI, useful for giving enterprises nearly instant insight to vital information for delivering IT services, ensuring information asset protection, and offering a strategy for continuous compliance.

Auditors, CIOs, CSOs, Compliance Managers and IT directors all recognize that to be effective, log management services require a complete LMI Platform that collects, aggregates, reports and alerts on, as well as safely stores all log data generated by the network.

LMI can automatically map data to control frameworks like CoBIT 4.1, ITIL and ISO 17799. By automating reporting and mapping to a framework, businesses can achieve compliance regulations like PCI, SOX, HIPAA and other common mandates on an ongoing basis, quickly and cost-effectively. LMI also lets companies customize frameworks to achieve broader business benefits.

Regulations Require LMI	Mandates Demand It	Controls Require It
SOX • FISMA • GLBA • JPA	PCI • SLAs • HIPAA	COBIT • ITIL • ISO
<p><b>NIST 800-53</b></p> <ul style="list-style-type: none"> <li>• Capture audit records</li> <li>• Regularly review audit records for unusual activity and violations</li> <li>• Automatically process audit records</li> <li>• Protect audit information from unauthorized deletion</li> <li>• Retain audit logs</li> </ul>	<p><b>PCI: Requirement 10</b></p> <ul style="list-style-type: none"> <li>• Logging and user activities tracking are critical</li> <li>• Automats and secure audits trails for event reconstruction</li> <li>• Review logs daily</li> <li>• Retain audit trail history for at least one year</li> </ul>	<p><b>COBIT 4.1</b></p> <ul style="list-style-type: none"> <li>• Provide audit trail root-cause analysis</li> <li>• Use logging to detect unusual or abnormal activities</li> <li>• Regularly review access, privileges, changes</li> <li>• Verify backup completion</li> </ul> <p><b>ISO 17799</b></p> <ul style="list-style-type: none"> <li>• Maintain audit logs for system access and use, changes, faults, corrections, capacity demands</li> <li>• Review the results of monitoring activities regularly and ensure the accuracy of logs</li> </ul>

“Get Fined, Go to Jail”      “Get Fined, Get Sanctioned”      “Lose Customers, Reputation, Revenue or Job”

## Features and benefits

- Provides “out-of-the-box” support for key regulations and IT governance frameworks.
- Allows organizations to use data to provide evidence of, and enforce IT controls.
- Automates compliance activities, such as sampling, and dramatically improves audit accuracy.
- Provides industry-leading reporting depth and breadth, including real-time reporting and alerting.
- Maintains immutable log data for investigation and litigation.
- Customizable to map data against company policies.
- Accelerates time to risk mitigation and audit response by searching terabytes of data in seconds.
- Allows data and reports to be accessed directly by end-users via Open Log Services; enables rapid creation of custom dashboards.

## Continuous Compliance

An integral part of its comprehensive LMI platform, LogLogic Compliance & Control Suites™ automate and simplify the process of using log data to evidence and enforce business and IT policies. With versions targeted for compliance with SOX, FISMA, HIPAA, PCI, and ISO 17799, LogLogic’s Compliance and Control Suites can be installed in minutes -- delivering results in seconds.

LogLogic’s Compliance Suites use LogLogic Agile Reporting™ technology to deliver more than 13,000 customized reports through 100+ reporting templates and alerts. IT staff can quickly customize templates to align with whatever IT control matrix, best practice standard and regulations are applicable to their business or industry.

By automating compliance reporting and alerting based on critical infrastructure data collected and stored by LogLogic’s appliances, LogLogic Compliance & Control Suites remove the complexity and resource requirements of implementing governance frameworks to successfully meet multiple regulatory regulations.

“Implementing new processes and policies in support of compliance has become a significant burden for IT departments worldwide. A key element of any such activity is collecting, storing, analyzing and reporting on log data. LogLogic’s Compliance Suites promise to reduce the costs and improve the accuracy of these initiatives.”

➤ Jon Oltsik  
Senior Analyst, Enterprise Strategy Group

## Universal Log Processing

Collect and process log data from any source.

## Agile Log Reporting

Create thousands of highly customized reports from 24 easy-to-use templates--as well as reports for FISMA, SOX, HIPAA, COBIT 4.1 and ISO 17799 frameworks--in seconds with no vendor intervention.

## Log Learning

Leverage powerful artificial intelligence and machine learning to set alerts based on changes to individual devices, groups of devices or the network.

## Log Forensics

Search terabytes of unaltered, unfiltered data in seconds—Indexing and “Google-like” search algorithms allow near-instant data retrieval.

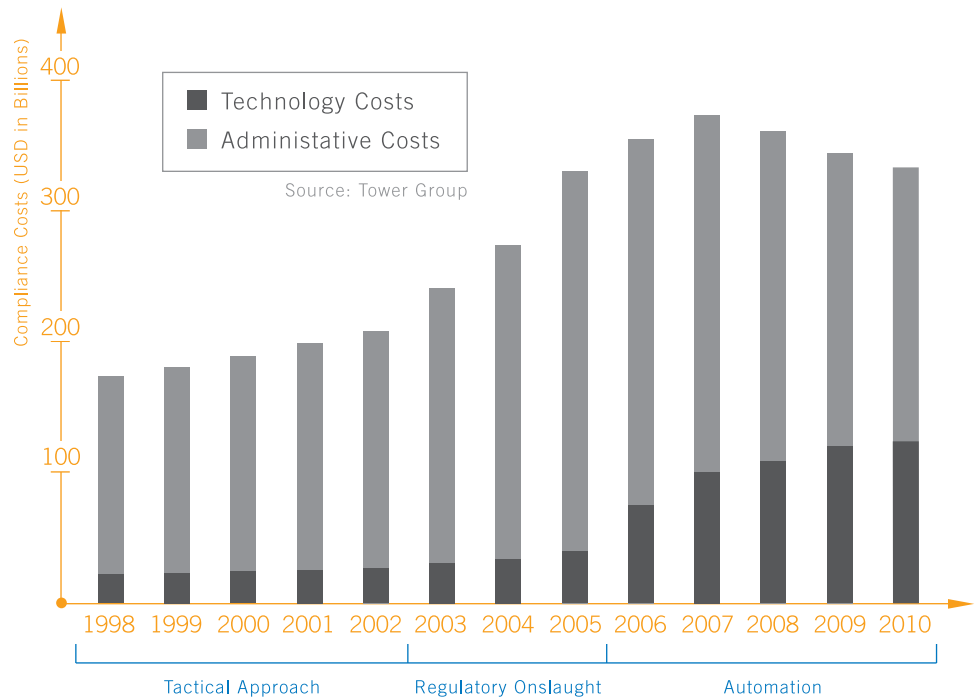
## Open Log Services

Easily route raw data, reports and alerts to existing SIEM, network management and trouble ticket or other solutions.

## Log Process Audit

Provide proof of compliance and critical information for legal proceedings during network activity audits.

Benefits of automating compliance activities go beyond reducing the burden that audits and investigations place on IT teams by implementing a strategy to achieve Continuous Compliance. With samples, reports, alerts and tools automated, the result is significantly reduced cost and complexity.



## Proving Forensics

Compliance and information protection mandates require more than simply generating trouble tickets; true incident response and the ability to quickly and thoroughly investigate and validate data are essential. Forensics is integral to the new generation of IT, and log management addresses this need quickly and cost effectively while removing the complexity.

LogLogic's LMI platform creates an immutable set of log data. From a compliance perspective, meta log data can't be modified or deleted, except according to set rules. In addition, log data must have controls for retention, access, movement and structure, to enable the creation of a complete chain of custody over your log data.

Rather than handling log management, records/reporting management, and log retention as separate processes or silos, an LMI platform combines these processes and procedures. In doing so, it provides a sustainable solution for compliance and forensics.

## Immutable Log Storage

At the heart of compliance, too, is immutable log storage. LogLogic solutions ensure:

- 1. No Logs Left Behind:** LogLogic's architecture enables all logs to be collected and stored.
- 2. Secure Storage and Transport:** Log data is secured not just when stored, but also in transport.
- 3. Chain of Custody:** LogLogic enhances the ability to achieve effective separation of duties by implementing controls over log data from applications, databases and operating systems.
- 4. Integrated and Integrateable:** Stores up to 24 TB of compressed log data on LogLogic, or uses your existing NAS and SAN.

## Installs In Minutes. Reports In Seconds.

LogLogic's pre-packaged Compliance and Control Suites enable enterprises to be up and running with compliance tasks in a matter of hours. LogLogic's award-winning appliances aggregate high volumes of log data and offer fast search and drill-down capabilities essential to rapid audit forensics, while automating log data archives and providing secure log data retention. Best of all, they are installed in just minutes. Using LogLogic technology, enterprises can consistently apply predefined business rules and perform complex calculations when processing large volumes of transactions or data. With LMI, IT staff can monitor the performance of all enterprise activities, policies and procedures.

## Greater Business Agility

LogLogic Compliance and Control Suites use Open Log Services to provide greater business agility and productivity through ease of integration of software component and application reuse. Based on the principals of a services-oriented architecture (SOA), LogLogic's Open Log Services enable intelligent data sharing with other applications and services, fueling greater insight into user, systems and network activity.

## Time-Saving Customization

Using LogLogic's Agile Reporting & Alerting™ technology, enterprises use log data to evidence and attest to controls and processes, proving and sustaining compliance at a fraction of the cost of alternate or homegrown solutions. Instead of having to write PERL scripts or SQL statements to customize reports, Agile Reports can be customized with a few clicks of the mouse. IT staff can develop custom dashboards based on industry-standard processes or their own reporting requirements. Open Log Services also enable raw data, alerts and reports to be easily routed to third-party management and compliance solutions to close the loop on, and constantly validate, business processes. LogLogic allows users to enhance the timeliness, availability and accuracy of information.

## Reliable Risk Mitigation

LogLogic's breakthrough Log Learning™ technology delivers the industry's first smart behavioral alerts, which can be set by device, device group or network. Adaptive baseline, network policy and ratio-based alerts are all powered by artificial intelligence and machine learning technology. Managers receive early warning of insider misuse, in addition to any unusual or suspicious behavior, so they can act quickly. Moreover, LogLogic significantly reduces the risk that controls will be circumvented.

## Rapid ROI

Companies stand to realize an ROI in just six months, based on reduced or eliminated consulting, personnel and infrastructure costs. Additionally, LogLogic's centralized management capabilities reduce data storage requirements and management costs. Completing compliance reporting is reduced by up to two weeks per report, freeing IT staff to concentrate on other business-critical tasks.

## LogLogic 4 with the LogLogic Compliance Suites

- **Collect 100% of all log data:** All data, 100% of the time, from any device, including network storage, servers and homegrown applications.
- **Store 100% Log Data Immutably:** As much as you need, as little as you want. Meet SOX compliance and security requirements with efficient and automated storage and archival of critical log data.
- **Out-of-the Box Reports:** 10 seconds to reporting following a 10-minute install. Proof of compliance using 100+ easy-to-use templates. Use the LogLogic Agile Reporting Engine to develop up to 13,000 custom reports. Easily align your log data reporting and IT control matrix.
- **Set Alerts for Continuous Compliance:** Develop your own alerts or choose from prepackaged alerts.

## Compliance Suites to Suit Your Business Needs

### COBIT 4.1 and SOX Compliance & Control Suite

The Sarbanes-Oxley Act (SOX) of 2002 safeguards against accounting errors and fraudulent management practices at publicly traded firms. The act holds CEOs and CFOs personally responsible for misrepresentation of company performance. Specifically, Section 404 establishes the need for internal controls based on a recognized control framework. To meet this requirement, effective log management is essential. LogLogic's COBIT 4.1 SOX Compliance Suite enables enterprises to use log data and intelligence to build an effective strategy for meeting these requirements.

### PCI Compliance & Control Suite

The Payment Card Industry Data Security Standard (PCI DSS Standard) aims to reduce cardholder fraud and maintain the reputation for trust and security of the leading credit card brands. It applies to all companies involved in handling credit card transactions and incorporates 12 basic requirements designed to secure and protect cardholder data from unauthorized access. With customized reports that map to PCI's 12 requirements, LogLogic's PCI Compliance Suite is a powerful resource for compliance with the PCI Standard, enabling merchants and service providers to gain greater visibility and security in their networks.

### HIPAA Compliance & Control Suite

The Health Information Portability and Accountability Act (HIPAA) provides for the confidentiality, integrity and availability of Protected Health Information. LogLogic's unique capabilities to collect, alert on, analyze, store and archive log data are essential for ensuring HIPAA compliance. With the LogLogic HIPAA Compliance Suite, health care organizations can prevent undesired access to sensitive patient data and rapidly remediate network issues that may affect patient care, all while reducing the costs of compliance through automation.

### FISMA Compliance & Control Suite

Government agencies recognize the critical role protecting information assets has on the security of our national infrastructure and the importance of best-in-class IT governance. A number of laws and regulations substantiate the mandate for log management and analysis in the government. The most pertinent of these is likely the Federal Information Security Management Act of 2002 (FISMA) and, specifically, Title III, Subchapter III, which deals with "Information Security." Most agencies recognize that there is a broader mandate to audit, monitor and alert appropriate personnel to address and reduce fundamental security and operational risks and to ensure compliance with service-level targets.

### ISO 17799

Recognized as an international information security standard that provides information management security recommendations to those in an organization responsible for security, ISO 17799 enables organizations to proactively identify weaknesses and threats before the auditor does.

LogLogic supports 100% of all log-related IT controls and best practices as outlined by ISO, significantly reducing the cost and complexities of compliance. LogLogic automates key ISO 17799 processes with Agile Reporting, allowing ISO 17999 reports to be easily generated from user-friendly templates.

### ITIL

The IT Infrastructure Library (ITIL) is a process-oriented IT control framework for service management organizations. Developed in the late 1980s by the United Kingdom's government, this framework has been widely adopted and is now the most accepted and used IT service management best practices approach in the world.

ITIL offers a process that enables the effective management of IT organizations. The popularity of ITIL and IT and business processes automation is fueled by two concurrent market forces resulting into a 'perfect storm' for ITIL and IT Service Management: The desire to reduce IT costs while maintaining and improving IT Service Quality and the requirement to create better control and visibility into IT for regulatory compliance.



[loglogic.com](http://loglogic.com)  
[blog.loglogic.com](http://blog.loglogic.com)  
[info@loglogic.com](mailto:info@loglogic.com)

LogLogic, Inc  
110 Rose Orchard Way  
San Jose, CA 95134  
United States  
US Toll Free: 888 347 3883  
Tel: +1 408 215 5900  
Fax: +1 408 321 8717

LogLogic EMEA  
Albany House  
Market Street  
Maidenhead, Berkshire SL6 8BE  
United Kingdom  
Tel: +44 870 351 7594  
Fax: +44 870 351 7595

LogLogic APAC  
Suite 303, Tower B, Beijing Kelun Building  
12A, Guang Hwa Lu  
Chaoyang District  
Beijing 100020, China  
Office: +8610 6581 3298  
Fax: +8610 6581 3299

---

LogLogic, Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Product Specifications are subject to change without notice.

©2007 LogLogic, Inc. All rights reserved. LogLogic is a trademark of LogLogic, Inc. All other products or services mentioned are the trademarks, service marks, registered trademarks or registered service marks of their respective owners.