

# LogLogic Compliance Suite: COBIT 4.1 and SOX Edition

Automate Reports & Alerts. Accelerate Time to Compliance.



The LogLogic Compliance Suite Instantly Turns Log Data Into Automated Reports and Alerts for Monitoring of IT controls, COBIT 4.1, SOX and more.

Enterprises recognize the critical role protecting information assets has on the success of their business and the importance of best-in-class corporate governance. The LogLogic Compliance Suite: COBIT 4.1 and Sarbanes-Oxley Edition enables best practices and processes to be easily implemented and enforced to support the IT governance requirements of executives and boards, while also addressing the more detailed requirements of those responsible for solution and service delivery. As a result, CIOs can optimize IT investments, ensure value delivery and mitigate IT risk in a transparent manner.

The LogLogic Compliance Suite automates the process of using log data to evidence and enforce business and IT policies such as Sarbanes-Oxley through COBIT 4.1, ITIL and more. The first solution of its kind, LogLogic's Compliance Suite delivers 100+ reports and 75+ alerts - both easily customizable - that run on LogLogic's award winning LogLogic 4 appliances.

Enterprise data in the form of log files provides critical insight into the use of corporate assets, risks and IT performance. In addition to servers and applications, much valuable information comes from mining the log data from corporate firewalls, databases, web proxies, IDS systems, E-mail servers and backup systems.

## Key Features and Benefits

- ▶ Allows organizations to use data to provide evidence of, and enforce IT controls.
- ▶ Automates compliance activities and dramatically improves audit accuracy.
- ▶ Provides industry-leading reporting depth and breadth, including real-time reporting and alerting on COBIT 4.1 for SOX compliance.
- ▶ Delivers sustainable compliance through real-time alerting – including 75+ alerts mapped to COBIT 4.1.
- ▶ Customize any report using LogLogic's Agile Reporting Engine to map data against your company's policies.
- ▶ Accelerates time to risk mitigation and audit response by searching terabytes of data in seconds.

Automating Compliance. Mitigating Risk.

) The Sarbanes-Oxley Act (SOX) of 2002 sets a standard for corporate accountability, requiring the definition and enforcement of internal controls and processes. It applies to all public companies. The Sarbanes-Oxley Act recommends companies regularly audit log files and keep a record of audit logs for up to seven years. SOX specifically requires companies to “audit unauthorized access, misuse and fraud, in order to ensure the accuracy of corporate financial and business information,” and to “maintain financial records for seven years.”

) To aid organizations in successfully meeting today's business challenges, the IT Governance Institute (ITGI) has published version 4.1 of Control Objectives for Information and related Technology (COBIT).

) COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations.

## 100+ Agile Reports. 75+ Alerts.

The LogLogic Compliance Suite is the first solution of its kind to provide “out-of-the-box” validation of COBIT 4.1 and ITIL. COBIT is the IT Governance Institutes IT governance and control framework, most frequently used to help achieve Sarbanes-Oxley Act compliance, but also ensuring security and availability of IT assets in general.

The COBIT controls and corresponding LogLogic reports and alerts cover six important areas of IT risk management:

- **Access:** Identity and access monitoring
- **Activity:** User activity monitoring
- **Change:** Change control monitoring
- **Security:** Security monitoring
- **Infrastructure:** IT infrastructure monitoring
- **Continuity:** Business continuity management

By automating compliance reporting and alerting based on critical infrastructure data collected and stored by LogLogic's series 4 appliances, the LogLogic Compliance Suite removes the complexity and resource requirements from implementing policies such as COBIT and ITIL to successfully meet SOX and other regulations.

## Customizable Compliance Reporting

The LogLogic Compliance Suite uses LogLogic's unique Agile Reporting Engine to allow on-the-fly customization of templates. Using Agile Reporting functionality, customers can match information from log data against specific corporate controls and policies. Agile Reporting differentiates LogLogic's compliance solution from industry alternatives based on static reports. Instead of having to write Perl scripts or SQL statements to customize reports, Agile Reports can be customized with a few simple mouse clicks.

## Real Alerts and Reports Based on Real Data

LogLogic Compliance Suite deliver reports and alerts on all four areas of the IT risk management framework defined by COBIT 4.1:

- **Plan and organize (PO):** This domain covers strategy and tactics, and identifying the way IT can best contribute to achieving business objectives.
- **Acquire and implement (AI):** To realize the IT strategy, IT solutions need to be identified, develop or acquired, as well United States as implemented and integrated into the business process.
- **Delivery and support (DS):** This domain is concerned with the actual delivery of required services, which includes service delivery, security and continuity management, service support for users, and data and operational facilities management.
- **Monitor and evaluate (ME):** All IT processes need to be regularly assessed over time for quality and compliance with control requirements. This domain addresses performance management, internal control monitoring, regulatory compliance and governance.

## LogLogic 4 with the LogLogic Compliance Suite

**Collect:** 100% of all log data, 100% of the time, from any device, including network storage, servers and homegrown applications.

**100% Pure Log Data Storage: 100% Pure Log Data Storage:**

security requirements with efficient and automated storage and archival of critical log data.

**100+ Reports For COBIT:** 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.

**Alert For Sustainable Compliance:** Develop your own alerts or use 75 prepackaged alerts based on COBIT. Automated alerts help mitigate risks and identify compliance and security threats in seconds.

Compliance reporting and alerting from LogLogic is ideal for IT administrators, auditors and financial executives who want to reduce time to compliance and realize dramatic improvements in risk mitigation and audit accuracy.

LogLogic allows for ongoing data monitoring and reporting and long-term archival so you can attest to compliance activities on an ongoing basis. 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 and unusual or suspicious behavior so they can act quickly.,

## Extensive Benefits. Rapid ROI.

With LogLogic's Compliance Suite, IT personnel can reduce the development and management of audits and reporting from weeks to an hour or less. With real-time alerting out of the box on key processes such as user authentication, access control and information protection, enterprises can achieve sustainable compliance with a fraction of the resources or risks of alternate solutions. Typical benefits for IT, auditors and financial executives include:

- Time reduction of up to two weeks per report and a dramatic improvement in risk mitigation and accuracy. ROI of 1-3 months based on reduced or eliminated consulting, personnel and infrastructure costs.
- Ease of attestation. Reports load in seconds and immediately start generating results on terabytes of log data.
- Sustainable compliance and a significant reduction in risk by delivering real-time, automated alerting on policies and controls.
- Log Process Auditing to automatically evidence that processes are being completed on time.
- Reduced data storage and management costs. Protection of the integrity of log data for purposes of attestation and litigation. Many current solutions (homegrown and security information and event management) damage and reduce infrastructure data when processing it. They also fail to deliver a way of systematically capturing and securely storing critical infrastructure data spread across the enterprise (and, of enforcing and evidencing this process).

### AGILE LOG REPORTING

Create up to 13,000 highly customized reports from 24 easy-to-use templates. Create reports for SOX, HIAA, COBIT 4.1 and ISO 17799 frameworks in seconds with no vendor intervention. 100+ reports and more than 75 alerts for COBIT and SOX.

### LOG LEARNING

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

### LOG FORENSICS

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

### OPEN LOG ROUTING

Routes raw data, reports and alerts to existing SIEM, network management, and trouble ticket/ other solutions.

### LOG PROCESS AUDIT

Enables network activity audits to provide proof of compliance or critical information for legal proceedings.



## Sample Controls Addressed by LogLogic for Sarbanes-Oxley Compliance

COBIT 4.1 can be downloaded from [www.isaca.org/cobit/](http://www.isaca.org/cobit/)

Category	COBIT 4.1	Control Header
Identity and Access	DS5.3	Identity management
	DS5.4	User account management
	PO7.8	Job change and termination
User Activity	PO4.11	Segregation of duties
	AI2.3	Application control and audit ability
Change	AI6.1	Change standards and procedures
	DS9.3	Configuration integrity review
Security	DS5.2	IT security plan
	DS5.5	Security testing, surveillance, monitoring
	DS5.10	Network security
	DS11.6	Security requirements for data mgmt
IT Infrastructure	DS1.5	Monitoring of service level agreements
	DS2.4	Supplier performance monitoring
	DS3.5	Monitoring of performance and capacity
	DS13.3	IT infrastructure monitoring
	DS10.2	Problem tracking and resolution
Business Continuity	DS4.1	IT continuity framework
	DS4.5	Testing of the IT continuity plan
	DS11.5	Backup and restoration

JOIN OUR WEEKLY  
DEMO AND FREQUENT  
WEBCASTS. >>

Visit [LogLogic.com](http://LogLogic.com)  
for more information.

**LogLogic, Inc.**  
110 Rose Orchard Way, Suite 200  
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  
Tel: +8610 6581-3298  
Fax: +8610 6581-3299



[www.altaware.com](http://www.altaware.com)  
[sales@altaware.com](mailto:sales@altaware.com)  
(866) 833-4070  
Your LogLogic Reseller

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



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.