TIBCO LogLogic Compliance Suite — FISMA Edition

BENEFITS

ENFORCES AND PROVIDES EVIDENCE OF IT CONTROLS

Uses system logs and other IT data to track performance, alert to unmet requirements, and formulate reports.

DRAMATICALLY IMPROVES AUDIT ACCURACY

Provides thorough industry-leading real-time reporting and alerting.

DELIVERS SUSTAINABLE COMPLIANCE

Helps automate compliance activities mapped to FISMA requirements.

PROVIDES FLEXIBILITY FOR FURTHER IMPROVEMENT

Provides customization of more than 300 reports and more than 100 alerts to support your company's policies.

AT A GLANCE

The Federal Information Security Management Act (FISMA) requires federal agencies to develop, document, and implement agency-wide programs to secure data and information systems supporting operations and assets, including those managed by other agencies or contractors. The TIBCO LogLogic® Compliance Suite – FISMA Edition uses logs to develop automated reports and alerts that help you meet FISMA requirements specific to log data and accelerate your drive to compliance.

FROM IT DATA TO INTELLIGENCE

The Compliance Suite's FISMA Edition enables best practices and processes to be easily implemented and enforced to support IT governance and service delivery. It uses data collected and stored by TIBCO LogLogic appliances — data including logs, flow data, and flat files — from applications, backup systems, databases, e-mail servers, firewalls, IDS systems, web proxies, and other systems. The data is filtered against specific corporate controls and policies to document adherence to FISMA compliance, as well as provide insight into performance, risk, and the use of corporate assets. Hundreds of reports and alerts can be customized on-the-fly to quickly provide needed information to IT and compliance staff.

RAPID ROI AND OTHER BENEFITS

With the LogLogic Compliance Suite — FISMA Edition, you can reduce time spent on developing compliance reports and managing audits from weeks to minutes. With out-of-the-box real-time alerting on key processes such as user authentication, access control, and information protection, agencies and organizations can achieve sustainable compliance with a fraction of the resources, and with less risk than alternate solutions. Typical benefits include:

COST SAVINGS

- Return on investment in 1–3 months based on reduced infrastructure costs and staff time and reduced or eliminated consulting expense.
- Reduced data storage and management costs.

TIME SAVINGS

- Reduced time designing and setting up reports.
- Easier attestation, with report fields customized in seconds and fast generation of results.

RISK MITIGATION

- Dramatic improvement in mitigating risk of non-compliance.
- Sustainable compliance by delivering real-time, automated alerting on policies and controls.

ATTRIBUTES & CAPABILITIES

Reports and alerts cover six important areas of IT risk management corresponding to FISMA controls:

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

FISMA EXAMPLES

CONTROL OBJECTIVE	SAMPLE REPORTS AND ALERTS
AC-2 Account Management	• Accounts Created/Deleted on Servers • Logins Succeeded, Failed Logins
AC-3 Access Enforcement	• Firewall Policy Changes • Logins Succeeded, Failed Logins
AC-6 Least Privilege	• Files Accessed on Servers • Escalated Privileged Activities
AC-7 Unsuccessful Login Attempts IA-2 User Identification	• Logins Succeeded, Failed Logins • Administrative Logins
AC-13 Supervision and Review/Access Control	• Accounts Created/Deleted on Servers • Windows Permission Modified
AC-17 Remote Access	• VPN User Accessing Corporate Network
AU-2/3 Auditable Events/ Content of Audit Records	• Log Sources Status • Windows Audit Logs Cleared
AU-5/6/7 Audit Monitoring and Reporting	• Periodic Review of Log Reports • Files Accessed on Servers
CM-3/4 Configuration Change Control/ Monitoring Configuration Changes	• Firewall Policy Changes • Windows Policy Modified
SC-7 Boundary Protection	• Firewall Traffic Considered Risky

TIBCO®

Global Headquarters
3307 Hillview Avenue
Palo Alto, CA 94304
+1 650-846-1000 TEL
+1 800-420-8450
+1 650-846-1005 FAX
www.tibco.com

06/29/17