ALERT LOGIC®

SOLUTION OVERVIEW:

ALERT LOGIC® FOR SOX COMPLIANCE

INTRODUCTION

The Sarbanes-Oxley Act (SOX) came into force in July 2002 and introduced major changes to the regulation of corporate governance and financial practice. By mandating the requirements for reliability and usefulness of financial reporting, SOX is designed to renew investor's trust and understanding of public corporation financial reporting.

SOX Section 404 mandates the management assessment over internal controls. For most organizations, internal controls span their information technology systems, which process and report the financial data of the company. The SOX Act provides specific details on IT and IT security. Many SOX auditors rely on standards, such as COBIT (Control Objectives for Information and Related Technology) as a method to gauge and audit proper IT governance and control.

ALERT LOGIC SOLUTIONS

Alert Logic simplifies IT security and compliance management by delivering an integrated solution consisting of Software-as-a-Service products and 24x7 Security Operations Center monitoring services for intrusion detection, vulnerability assessment, log management, and web application security. Our tightly integrated solutions enable our customers to seamlessly address the most costly and painful requirements of expanding compliance mandates, including SOX requirements, while lowering costs and accelerating deployment – whether the IT infrastructure resides in-house or in the cloud.

Alert Logic ActiveWatch and LogReview services provide expert human analysis, review and insight on real-time security threats and alerts. Additionally, these services satisfy compliance requirements for daily log review or 24x7 monitoring at a fraction of the cost of employing these skills in-house. This service increases the accuracy of threat detection, reduces false positives and allows you to stay focused on your business and lets you leverage expert analysts to alert you when suspicious activity is discovered.

SOX (COBIT) REQUIREMENTS

CJIS SECURITY POLICY (VERSION 5.2) POLICY		ALERT LOGIC SOLUTION
DS 5.5: Security Testing, Surveillance and Monitoring	• Ensure that IT security implementation is tested and monitored proactively.	Alert Logic Log Manager & Log Review service enables the early detection of unusual or abnormal activities that may need to be addressed. Log Manager enables: • Agentless or agent-based log collection and storage from syslog, Windows and text logs. • Automated correlation and alerting of defined security and compliance incidents. • Mandate-specific scorecards, dashboards & reporting.
DS 5.9: Malicious Software Prevention, Detection and Correction	• Ensure that preventive, detective and corrective measure are in place across the organization to protect information systems and technology from malware.	Threat Manager product provides the ability for scanning internal and external hosts for known vulnerabilities/missing patches and detects security incidents. It also includes a knowledge base for remediation steps. It detects and alerts to security events and incidents as they happen.
DS 13.3: IT Infrastructure Monitoring	• Define and implement procedures to monitor the IT infrastructure and related events. Ensure sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.	Alert Logic provides support for identifying systems and their roles that might have otherwise been not accounted for. The service provides daily review, analysis & monitoring of log reports by in-house GIAC certified security analysts
DS 5.6: Security Incident Definition	• Clearly define and communicate the characteristics of potential security incidents so that they can be properly classified and treated by the incident and problem management process.	Alert Logic identifies the potential security breaches or attempts to breach and helps the customer to mitigate the threat & suggests defensive methodologies or technologies to prevent future failures.

AI3.2: Infrastructure resource protection and availability	• Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined monitored and evaluated.	Alert Logic's Log Manager product identifies access to and usage of sensitive infrastructure and can be reviewed on a daily basis with the Log Review service.

ABOUT ALERT LOGIC

Alert Logic, the leader in security and compliance solutions for the cloud, provides Security-as-a-Service for on-premises, cloud, and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Fully managed by a team of experts, the Alert Logic Security-as-a-Service solution provides network, system and web application protection immediately, wherever your IT infrastructure resides. Alert Logic partners with the leading cloud platforms and hosting providers to protect over 3,500 organizations worldwide. Built for cloud scale, our patented platform stores petabytes of data, analyses over 400 million events and identifies over 50,000 security incidents each month, which are managed by our 24x7 Security Operations Center. Alert Logic, founded in 2002, is headquartered in Houston, Texas, with offices in Seattle, Dallas, Cardiff, Belfast and London. For more information, please visit www.alertlogic.com.

ALERT LOGIC®