SOX Compliance Management
Configuration Management Systems

Configure Consulting Inc.
by Brian Wong
Practice Lead - Security & Compliance
October 2012

SOX Compliance
Management

Ensuring the corporate electronic financial documents cannot be tampered with is an important technical requirement in remaining a SOX compliant institution. A seemingly confusing series of technical specifications and procedures must be adhered to. Configure Consulting specializes in implementing a CMS (configuration management system) solution to provide the visibility and audit capability required to validate SOX compliancy. Below are common SOX security requirements that this suite of tools can assist your organization in achieving.

Manage Firewall Configuration Settings

SOX compliancy dictates that firewalls should only allow http and https ports except when applications such as FTP are in use. Configure Consulting has implemented CI policies to automatically report on the IP Service Endpoints detected on any given firewall. Any endpoints other than 80 (http) and 443 (https) should flag a breach of security.

Enforce External Web Server and Internal Network Boundaries

Having an external facing web server be separate from the internal network is a rule of thumb for most enterprises, and is crucial in remaining SOX compliant for SOX applications. Our suggestion for clients across North America has been to align configuration policy management with automated infrastructure discovery to proactively detect any policy breaches and systemic risks. If a mapped application web server and application or database server reside on the same network, the system flags a breach.

Manage Database Port Security

Gain insight into the database remote listening ports used in your IT environment with CMS to discover all IP service endpoints. To remain SOX compliant databases should listen on non-default ports. With configuration management policy it is easy to flag a breach when a default port is discovered on a SOX configuration item (CI).

Configure Consulting

Practice Reasonable and Secure ID Management

Gain insight into the user accounts that are available on discovered systems. It is not reasonable to have guest accounts or user accounts without passwords or administrative accounts with default passwords on any system with relationships to SOX applications. Ensure only secure accounts and credentials are available for use and become notified should an unauthorized user account be created on any system.

Maintain Compliancy

Once a reasonable and documentable computer security policy has been implemented, it must be maintained. Automated discovery results are routinely compared against baseline of all existing compliant hardware, software and network components - with automated notification of any compliance breaches.

For more Information

To learn more about proactive compliance solutions, secure ID management, configuration and change management contact the Configure Consulting team at 1-800-987-8460 or info@configureconsulting.com.

About Configure Consulting Inc.

Configure Consulting implements quick-start solutions to empower IT operations teams with the efficiency, stability and top performance in the delivery of business services. Configure Consulting has been installing solutions globally for Fortune 500 clients across a number of industries. Configure Consulting has particular expertise with change configuration and release management, closed-loop incident process, business service management, configuration management systems, and service asset and configuration management.

After a successful implementation, our clients come away with leading solutions following industry best practices. The Configure Consulting team has developed a deep understanding across the HP IT Performance Suite (formerly BTO) portfolio and has attained HP ExpertONE certifications. The close partnership with the customer through each step of the implementation provides with a high quality solution.