CONSENTRY NETWORKS COMPLIANCE MATRIX

FOR SARBANES-OXLEY SECTION 404

The table below identifies specific objectives outlined within the CobiT Framework for Sarbanes-Oxley Section 404 compliance and the ConSentry product features that address those objectives.

CobiT Framework IT Processes	Overview of Control Objectives	What the ConSentry Solution Offers
Planning and Organization		
2.0 Define the information architecture	Develop information architecture model, data dictionary, classification scheme and security levels	Allows IT to define policies around network and information access and enforce those policies in an integrated/ turnkey device
8.0 Ensure compliance with external requirements	Review external requirements (safety, privacy,e-commerce, insurance, etc.) and develop practices to comply with them	Allows for the creation of network and application access policies to ensure proper policy definition, enforcement, and audit
9.0 Assess Risks	Assess, identify and measure risks; develop action plans and risk acceptance standards	Provides a robust monitoring application that provides up-to-the-minute views on organizational security issues and risks. These risks are associated with user groups and roles within the organization.
Delivery & Support		
1.0 Define and manage service levels	Determine adequate performance for service levels; monitor and report on that performance	Provides, in a future release, robust rate limiting and traffic prioritization [802.1p, IPTOS] which will help ensure service levels for priority traffic
3.0 Manage performance and capacity	Determine plans and requirements for system availability and performance	Provides detailed information on user and user group usage of the network and resources. This data can be utilized for traffic flow analysis and bandwidth capacity planning
5.0 Ensure systems security	Take necessary steps to secure the system, including identification, authentication, online access, account management, surveillance, data classification, rights management, incident handling, malicious software, firewall architectures and more	Enables granular policy management of which applications users may run. The system can be configured to automatically block a user or user group from running an unallowed application
6.0 Identify and allocate costs	Determine chargeable items and costing and billing procedures	Provides granular feedback on resource and application usage on a per group basis, and can be utilized for charge backs to internal divisions or customers

CobiT Framework IT Processes	Overview of Control Objectives	What the ConSentry Solution Offers
9.0 Manage the configuration	Record and manage system configuration, including procedures for unauthorized software, software storage and accountability	Works in conjunction with various host posture checking agents and will allow/deny network access based on compliance to the stated policy. In addition, the ConSentry products feature an optional host posture agent integrated into our platform that can deliver a disolvable agent to any system that is attempting to access the network and conduct a compliance scan on the system to determine if it adheres to the corporate configuration standards
10.0 Manage problems and incidents	Design a problem and emergency management system	Contains complete audit trails of individual user activity on the network. The system automatically binds user identity [user name, IP address, MAC address] to L7 application
11.0 Manage data	Develop procedures for source document, authorization, collection error handling and retention data processing integrity, validation, editing and error handling; output handling, retention, distribution, balancing, reconciliation, review and error handling; security provisions for output and sensitive information transmission; media library management; back-up restoration and storage; and protection of sensitive messages	Contains complete audit trails of individual user activity on the network. The system automatically binds user identity [user name, IP address, MAC address] to L7 application
Monitoring		
2.0 Assess internal control adequacy	Monitor the operation of internal controls and report on their effectiveness	Maintains complete audit trails of individual user activity on the network. The system automatically binds user identity [user name, IP address, MAC address] to L7 application
3.0 Obtain independent assurance	Certify and accredit IT services and third-party service providers; evaluate IT and third-party effectiveness independently; assure IT and third-party compliance with laws, regulatory requirements and contracts; conduct proactive audits	Maintains complete audit trails of individual user activity on the network. The system automatically binds user identity [user name, IP address, MAC address] to L7 application

CONSENTRY NETWORKS

ConSentry Networks
1690 McCandless Drive
Milpitas CA 95035

Phone 408.956.2100 **Fax** 408.956.2199
Toll-Free 866.841.9100
Email info@consentry.com
www.consentry.com