



Tufin SecureTrack and Sarbanes-Oxley Compliance

A White Paper by Tufin Technologies
June 2005

Introduction

The Sarbanes-Oxley Act (SOX) was enacted by the U.S. Congress in 2002 in order to provide greater accountability in Public Companies. The driving forces behind SOX are the corporate accounting scandals of Enron, Worldcom, and others. In the wake of these debacles, US Senators Paul Sarbanes and Michael Oxley architected the SOX legislation in order to reduce fraud and restore public investor confidence, by increasing transparency and providing controls over financial operations and accounting.

Although most of the Act applies to financial controls, significant parts of it are relevant to IT infrastructure, and in particular IT security. Most large U.S. companies find compliance with SOX quite challenging, as its implementation requires many changes in both financial and IT processes.

Tufin SecureTrack provides several key components of IT security controls required for SOX compliance. This whitepaper serves as an overview of SOX requirements and their implementation in SecureTrack.

Defining SOX Requirements

SOX legislation does not define effective internal controls since these depend on the company's business and structure, and may vary greatly from company to company. However, in June 2003, the Securities and Exchange Commission (SEC) published its final rules for SOX, and identified the Committee of Sponsoring Organizations (COSO) internal control framework as a set of criteria that can be used as guidance in the evaluation and development of controls. COSO is an organization whose purpose is the improvement of financial reporting standards. It is sponsored by different organizations, including the American Accounting Association, the Institute of Internal Auditors, and others.

The COSO framework for internal controls includes five elements: Control Environment, Risk Assessment, Control Activities, Information and Communication and Monitoring. Even though these elements sound like IT security controls, COSO is an accounting standard, not an IT standard. It focuses on reporting and controls for accounting, and not for IT security processes.

In the absence of direct guidance from the SEC or COSO, companies have turned to Industry "Best Practice" guidelines and frameworks of IT standards in order to design and implement effective IT security control. The most prominent framework used by companies today is Control Objectives for Information and related Technology (COBIT) published by the IT Governance Institute.

The COBIT Framework

The 3rd edition of COBIT provides the details necessary for IT controls to meet SOX requirements.

The COBIT framework helps to meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. It provides a set of best practice guidelines within a process framework and presents activities in a logical and easy-to-follow structure. COBIT's best practice guidelines reflect the cumulative work of many security experts, and incorporate requirements from different security frameworks, such as ISO 17799.

COBIT provides a set of 34 high-level control objectives, one for each of the IT processes, grouped into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring. This structure covers all aspects of information and the

technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment.

The Role of SecureTrack in IT Security Operations

Tufin SecureTrack plays a vital role in the success of IT security methodologies, providing critical elements of tracking, monitoring and analysis of changes in security configurations.

As business and IT managers devise practices and procedures that ensure compliance with internal and external regulations, SecureTrack's Organizational Policy provides a logical framework for defining high-level policies for changes in Firewall policy. Best practice guidelines for security policies can be easily applied and enforced as part of the real-time policy audit. Business and IT managers can use SecureTrack's compliance framework to align security policies with business objectives and external requirements, achieving a key element of SOX compliance.

In addition, SecureTrack's Organizational Policy compliance framework provides a platform for risk management, which enables detailed risk level specification for various policy change events.

Some examples of organizational policy alert rules include:

- Changes to specific High Risk rules (e.g., cleanup rule, DMZ rule, etc).
- Changes made outside normal hours of operation
- Changes made to traffic rules between the certain networks
- Rules added that contain Any in the source or destination, and Accept as action
- Changes to VPN rules
- Rules enabling peer-to-peer and file-sharing protocols
- Changes to Global Properties

Any violation of the Organizational Policy triggers real-time alerts, which are sent to IT managers and security officers. By providing the means to define and enforce risk levels for security-related administrator activities, SecureTrack delivers advanced risk identification and mitigation. Besides the obvious security benefits, this unique capability satisfies COBIT guidelines for risk identification and security surveillance.

Once the IT department implements proper procedures for change management, SecureTrack provides the means for IT managers to maintain complete control over security policy changes. SecureTrack constantly monitors Firewall configurations, and alerts registered users on policy changes in real-time, via email, SysLog and SNMP traps. Every policy revision is stored in SecureTrack's internal database, with a long-term storage capacity of several years' worth of policy change data. Detailed, real-time policy change reporting achieves full compliance with COBIT guidelines for change control and configuration control.

Key COBIT Guidelines and SecureTrack

The following table provides a mapping between specific COBIT 3rd edition guidelines and their implementation in SecureTrack:

| COBIT Section - Planning & Organization | |
|--|---|
| COBIT Objective | SecureTrack Solution |
| <p>PO 8.2 – Practices and Procedures for Complying with External Requirements Plan practices and procedures for compliance with external requirements, such as regulations, standards, laws, and requirements from business partners and customers.</p> | <p>SecureTrack's Organizational Compliance Policy enables fine-grained compliance auditing for Security Policy changes. The intuitive compliance definition interface assists IT managers in planning a comprehensive security practices framework.</p> |

| | |
|---|--|
| <p>PO 8.4 – Privacy, Intellectual Property and Data Flow Ensure compliance with privacy, intellectual property, trans-border data flow and cryptographic regulations applicable to the IT practices of the organization.</p> | <p>Using SecureTrack's Compliance Audit, SecureTrack can alert Security Officers on changes in the VPN policy, and violations of specific inter-network communication limitations.</p> |
| <p>PO 9.3 – Risk Identification Define a process for risk assessment and cause/effect relationship.</p> | <p>Organizations can assess the risk associated with Security Policy changes by tracking policy changes in real-time and monitoring violations of the Organizational Policy.</p> |

| COBIT Section - Acquisition & Implementation | |
|--|---|
| COBIT Objective | SecureTrack Solution |
| <p>AI 6.3 – Control of Changes Ensure proper integration between change management, software control and distribution and a comprehensive configuration management system. The monitoring system should be automated to support the recording and tracking of changes made to large, complex information systems.</p> | <p>SecureTrack monitors the Firewall configuration and includes mechanisms for automated, continuous change tracking. It integrates with various change monitoring frameworks to provide a unified change and configuration management interface.</p> |

| COBIT Section - Delivery & Support | |
|---|--|
| COBIT Objective | SecureTrack Solution |
| <p>DS 5.7 – Security Surveillance Security activity should be logged and any security violations should be reported immediately to all relevant parties, internally and externally, in a timely manner.</p> | <p>Security Policy changes and violations are logged and stored in SecureTrack's revision database. Alerts are sent via email, SysLog or SNMP traps.</p> |
| <p>DS 5.10 – Security Violation Reports Security violations and activities should be logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity.</p> | <p>Organizations can use SecureTrack's detailed reports and Compliance Policy alerts to review changes and quickly escalate them. Historical activity reports enable Security Officers to examine policy change activity using a variety of criteria.</p> |
| <p>DS 5.11 – Incident Handling A centralized computer incident-handling platform should be established to address security incidents by providing with sufficient expertise and equipped with rapid and secure communication facilities.</p> | <p>SecureTrack can be used to minimize the effects of network downtime caused by configuration errors. During a downtime event incident, administrators can use the side-by-side graphical comparison to identify and quickly resolve the erroneous changes, and restore normal network operation.</p> |
| <p>DS 9.4 – Configuration Control Procedures should ensure that the existence and consistency of recording of the IT configuration is periodically checked.</p> | <p>SecureTrack can send out periodic status indications (keep-alive) via SNMP traps, to ensure its proper operation and connection to the Firewall Management servers.</p> |
| <p>DS 9.7 – Configuration Management Procedures Configuration management procedures should be established to ensure that critical components of the organization's IT resources have been appropriately identified and are maintained.</p> | <p>SecureTrack's Firewall Policy Revision Control, policy change reports and graphical comparison view provide effective configuration management for an organization's Firewall Policy.</p> |

| | |
|--|---|
| DS 10.3 – Problem Tracking and Audit Trail The problem management system should provide for adequate audit trail facilities, which allow tracing from incident to underlying cause and back. | SecureTrack can easily distinguish the Administrator responsible for a certain policy change, providing a “root cause” analysis for incidents resulting from Firewall policy changes. |
|--|---|

Conclusions

Many organizations are focusing significant efforts on improving IT operations and processes in recent years. Government regulations, such as Sarbanes-Oxley, increase the pressure on IT managers to achieve compliance in a short period of time. Most organizations use best practice frameworks to achieve compliance, such as COBIT.

Tufin SecureTrack enables auditing, monitoring and compliance with organizational policies, which are critical elements for Sarbanes-Oxley compliance in IT organizations. Using SecureTrack, organizations have the means to achieve a high level of control over security operations, align business and IT requirements, and enable world-class IT security operations.

More Information

SEC Final Rule on for Section 404 of SOX:
<http://www.sec.gov/rules/final/33-8238.htm>

COSO Framework organization:
<http://www.coso.org>

COBIT Framework (IT Governance Institute)
<http://www.itgi.org>

COBIT Information (Information Systems Audit and Control Association)
<http://www.isaca.org>