IPScan and Sarbanes-Oxley Compliance

Implementing Compliant Internal Network Access Controls

ViAScope USA

Executive Summary

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. IPScan 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 IPScan.

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 COBIT framework, now in its 3rd edition, provides the details necessary for IT controls to meet SOX requirements. The COBIT framework helps companies 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 IPScan in IT Security Operations

ViaScope IPScan plays a vital role in the success of IT security methodologies by applying real-time, network-wide controls and auditing of fundamental Ethernet and IP network access. IPScan closes a significant gap in internal IT security and controls, to help organizations ensure that the internal Ethernet/IP network itself is not a ready source of internal security breaches. By deploying IPScan, organizations can win back control over access into their networks. The IPScan solution provides 99.9% Ethernet/IP access control and audit trail capabilities for SOX compliance. It also offers centralized management over an unlimited number of locations and devices. All access to the network and unauthorized attempts can be documented via the feature rich reporting capabilities within IPScan for a complete audit trail that meets the guidelines for SOX compliance.

The benefits of having effective internal controls in place go beyond SOX compliance. Having strong controls in place can make businesses more competitive, efficient, and less open to risks. With IPScan managing all IP/MAC addresses automatically, profitability can be increased through reduced IT operating expenses. Since it blocks duplicate IP addresses and protects critical network components, costly network disruptions can be avoided. Furthermore, the benefits of real-time internal monitoring and active security are of paramount importance to any organization.

Key COBIT Guidelines and IPScan

The following table provides a mapping between specific COBIT 3rd edition guidelines and IPScan's capabilities.

COBIT Section: Planning and Organization	
COBIT Objective	**IPScan Solution Capabilities**
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.	IPScan's network-wide access and address control policies enable global, yet fine-grained configuration, monitoring, enforcement and auditing of internal network security policies for compliance purposes.
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.	Using IPScan, network and security officers can be alerted to any unauthorized access attempted on the enterprise-wide Ethernet and IP backbone network.
PO 9.3 – Risk Identification: Define a process for risk assessment and cause/effect relationship.	Organizations can assess the risk associated with policy changes by tracking their enforcement in real-time and monitoring attempted violations of the organization's network access policy.

COBIT Section: Acquisition and Implementation	
COBIT Objective	**IPScan Solution Capabilities**
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.	IPScan monitors and enforces network access policy in real-time across the entire network, so that policy change is never disjoint from policy enforcement in the network. In addition, all device access changes are recorded for audit trails over time.

COBIT Section: Delivery and Support	
COBIT Objective	**IPScan Solution Capabilities**
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.	IPScan monitors, alerts, enforces and records all access to the network, including unauthorized attempts.
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.	Organizations can use IPScan detailed user/device reports and real-time alerts to review attempted access violations and quickly escalate them. Historical activity reports enable security officers to examine policy change activity.
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.	IPScan can be used to prevent downtime from IP address conflicts caused by unauthorized access attempts.
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.	IPScan allows network managers to view network access policy changes on an intuitive centralized console.
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.	IPScan can provide invaluable root cause analysis information of network issues caused by unauthorized access, by providing a complete audit trail of network device usage.

Conclusion

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, such as COBIT, to achieve compliance.

IPScan enables real-time, network-wide Ethernet/IP access and address control, including policy configuration, network-wide monitoring, real-time enforcement, and complete audit trail capabilities. IPScan offers IT organizations a significant enhancement in internal controls for SOX compliance, particularly protecting the network against internal security breaches that are a significant threat to sensitive data.

For more information on ViaScope and IPScan, please visit our website at: http://www.viascope.com, or send email to sales@viascopeus.com.