

Questions?

For more information:
408.213.3191
sales@forescout.com

Regulatory Compliance for Enterprise IT Security

Regulatory compliance has become a daunting task for most IT departments. Although the Sarbanes-Oxley Act (SOX) of 2002 mandates a comprehensive accounting framework for all public companies doing business in the U.S., there are specific requirements built into the legislation that govern IT policies, controls and security.

SOX is comprised of eleven main titles, further divided into sixty six sections. While the majority of the Sarbanes-Oxley Act focuses on checks and balances at the highest levels of an organization, two of the 36 sections have specific ramifications for IT security. These include:

Section 404(a) - Internal Control Reports

Each annual report must include an "internal control report" stating that management is responsible for an adequate internal control structure and an assessment by management of the control structure's effectiveness.

Section 404(b) - External Auditor Attestation Related to Internal Controls

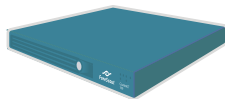
The accounting firm must attest to, and report on, management's assertions regarding its assessment of the effectiveness of the company's internal controls.

Section 409 - Real-Time Disclosure

Corporations will be required to disclose, on a rapid and current basis (48 hours), additional information concerning material changes in its financial condition or operations.

Since the enactment of Sarbanes-Oxley, most independent auditing firms have looked to The Control Objectives for Information and Related Technology (COBIT) for guidance in evaluating IT control frameworks. Released in 1992, COBIT is a platform-independent amalgam of many existing IT technical control frameworks, written from a business management perspective.

The COBIT framework specifies 34 high-level control objectives, broken down into 318 detailed objectives for a complete IT governance control program. These objectives range from establishment of oversight committees to the physical security of the facility. Of these requirements there are two primary sections that deal with intrusion prevention and incident escalation. Although there is no "silver bullet" that covers all requirements, ForeScout's appliances provide customers with a solution that fulfills several of the major criteria. The chart on the next page identifies some of the critical areas in which ForeScout's security appliance provides SOX compliance using the COBIT IT framework.



CounterACT: Proactive defense inside the enterprise network. Instantly identify and contain espionage and self-propagating threats before they compromise your network.



CounterACT Edge – Proactive defense at the enterprise network perimeter. Instantly stop threats from breaching your perimeter by identifying malicious sources and automatically blocking them at the source.

COBIT DS5 – Ensure Systems Security		
DS5.2 – Identification, Authentication, and Access	The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple logins. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).	In addition to typical authentication, ForeScout's CounterACT 5.0 Active Network Integrity module provides policy based network access based upon pre defined security criteria.
DS5.6 – User Control of User Accounts	Users should systematically control the activity of their proper account(s). Also, information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.	ForeScout appliances monitor data traffic and blocks/quarantines malicious activity. Notification of security event is immediate.
DS5.7 – Security Surveillance	IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.	ForeScout appliances retain a detailed log of malicious traffic as well as security policy violations.
DS5.9 – Central Identification and Access Rights Management	Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.	ForeScout's CounterACT 5.0 Network Information Portal provides a search engine capable of correlating information on network resources.
DS5.10 – Violation and Security Activity Reports	IT security administration should ensure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify, and resolve incidents involving unauthorized activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege, or need-to know.	ForeScout appliances retain a detailed log of malicious traffic as well as security policy violations. Reports can be generated detailing all security violations.
DS5.11 – Incident Handling	Management should establish a computer security incident handling capability to address security incidents by providing a centralized platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective, and timely response to security incidents.	In addition to organizational processes, ForeScout appliances can automate security event (malicious code, espionage, or policy violation) escalation through integration with trouble ticketing system.
DS5.17 – Protection of Security Functions	All security related hardware and software should at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. In addition, organizations should keep a low profile about their security design, but should not base their security on the design being secret.	ForeScout appliances are hardened and secured with the most advanced security and encryption technologies
DS5.19 – Malicious Software Prevention, Detection, and Correction	Regarding malicious software, such as computer viruses or Trojan horses, management should establish a framework of adequate preventative, detective, and corrective control measures, and occurrence response and reporting. Business and IT management should ensure that procedures are established across the organization to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response, and reporting.	ForeScout's patented ActiveResponse technology uses a deterministic approach to accurately and automatically identify and block self propagating malware BEFORE it penetrates the network.
DS5.20 – Firewall Architectures and Connections with Public Networks	If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and any unauthorized access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of service attacks.	ForeScout appliances augment existing firewall technologies by enabling real-time dynamic blocking of known and unknown threats.
COBIT DS10 – Manage Problems And Incidents		
DS10.2 – Problem Escalation	IT management should define and implement problem escalation procedures to ensure that identified problems are solved in the most efficient way on a timely basis. These procedures should ensure that these priorities are appropriately set. The procedures should also document the escalation process for the activation of the IT continuity plan.	ForeScout appliances can automate security event (malicious code, espionage, or policy violation) escalation through integration with trouble ticketing system.
DS10.3 – Problem Tracking and Audit Trail	The problem management system should provide for adequate audit trail facilities that allow tracing from incident to underlying cause (e.g., package release or urgent change implementation) and back. It should work closely with change management, availability management, and configuration management.	ForeScout captures all data related to the security event. Data can be easily exported for forensics and auditing.

